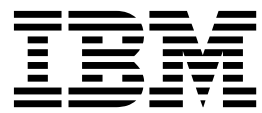


IBM Security AppScan Source for Analysis  
Versión 9.0.3.7

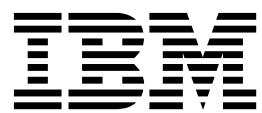
*Guía del usuario*





IBM Security AppScan Source for Analysis  
Versión 9.0.3.7

*Guía del usuario*



(C) Copyright IBM Corp. y sus licenciantes 2003, 2017. Reservados todos los derechos.

IBM, el logotipo de IBM, ibm.com Rational, AppScan, Rational Team Concert, WebSphere y ClearQuest son marcas registradas de International Business Machines Corp., registradas en muchas jurisdicciones del mundo. Otros productos y nombres del servicio pueden ser marcas registradas de IBM u otras compañías. Encontrará una lista actual de marcas registradas de IBM en el sitio web de Copyright and trademark information en <http://www.ibm.com/legal/copytrade.shtml>. Linux es una marca registrada de Linus Torvalds, Inc. en los Estados Unidos y/o en otros países. Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en Estados Unidos y/o en otros países. Unix es una marca registrada de The Open Group en los Estados Unidos y/o en otros países. Java y todas las marcas comerciales basadas en Java son marcas comerciales o marcas registradas de Oracle y/o sus filiales.

Este programa incluye: Jacorb 2.3.0, Copyright 1997-2006 The JacORB project; y XOM1.0d22, Copyright 2003 Elliotte Rusty Harold; cada uno está disponible bajo la licencia Gnu Library General Public License (LGPL) y una copia de la misma está disponible en el archivo de avisos que acompaña a este programa.

# Contenido

## Capítulo 1. Introducción a AppScan

### Source for Analysis. . . . . 1

|                                                                                        |    |
|----------------------------------------------------------------------------------------|----|
| Introducción a IBM Security AppScan Source . . . . .                                   | 1  |
| Cumplimiento de las regulaciones del Gobierno de los Estados Unidos . . . . .          | 2  |
| Novedades de AppScan Source . . . . .                                                  | 4  |
| Novedades en AppScan Source Versión 9.0.3.7 . . . . .                                  | 4  |
| Novedades en AppScan Source Versión 9.0.3.6 . . . . .                                  | 5  |
| Novedades en AppScan Source Versión 9.0.3.5 . . . . .                                  | 5  |
| Novedades en AppScan Source Versión 9.0.3.4 . . . . .                                  | 6  |
| Novedades de AppScan Source Versión 9.0.3.3 . . . . .                                  | 8  |
| Novedades en AppScan Source Versión 9.0.3.2 . . . . .                                  | 10 |
| Novedades de AppScan Source Versión 9.0.3.1 . . . . .                                  | 10 |
| Novedades de AppScan Source Versión 9.0.3 . . . . .                                    | 11 |
| Migración a la versión actual de AppScan Source. . . . .                               | 15 |
| Migración desde la Versión 9.0.2 . . . . .                                             | 15 |
| Migración desde la versión 9.0 . . . . .                                               | 16 |
| Migración desde la versión 8.7 . . . . .                                               | 17 |
| Visión general de AppScan Source for Analysis . . . . .                                | 19 |
| Flujo de trabajo . . . . .                                                             | 19 |
| Conceptos importantes . . . . .                                                        | 20 |
| Clasificaciones . . . . .                                                              | 21 |
| Inicio de sesión en AppScan Enterprise Server desde productos AppScan Source . . . . . | 21 |
| Habilitación de la autenticación con CAC (Common Access Card) . . . . .                | 24 |
| Modificación de las contraseñas de usuario de AppScan Source . . . . .                 | 26 |
| Certificados SSL de AppScan Enterprise Server . . . . .                                | 26 |
| AppScan Source y accesibilidad . . . . .                                               | 27 |
| Avisos . . . . .                                                                       | 28 |
| Copyright . . . . .                                                                    | 31 |

## Capítulo 2. Configuración de aplicaciones y proyectos . . . . . 33

|                                                                                                                                                     |    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Archivos de aplicación y de proyecto de AppScan Source . . . . .                                                                                    | 33 |
| Configuración de aplicaciones . . . . .                                                                                                             | 36 |
| Creación de una nueva aplicación con el Asistente para aplicaciones nuevas . . . . .                                                                | 37 |
| Utilización de Application Discovery Assistant para crear aplicaciones y proyectos . . . . .                                                        | 38 |
| Adición de una aplicación existente . . . . .                                                                                                       | 41 |
| Adición de varias aplicaciones . . . . .                                                                                                            | 43 |
| Importación de las aplicaciones Java desde Apache Tomcat y los servidores de aplicaciones de WebSphere Application Server Liberty Profile . . . . . | 44 |
| Adición de un espacio de trabajo de Eclipse o de un producto basado en Eclipse . . . . .                                                            | 46 |
| Configuración del entorno de desarrollo para proyectos de Eclipse y Rational Application Developer for WebSphere Software (RAD) . . . . .           | 47 |
| Actualizaciones de Eclipse o Application Developer . . . . .                                                                                        | 47 |

|                                                                                                                                                                  |    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Importadores del espacio de trabajo de Eclipse: configuración de preferencias de Eclipse o Rational Application Developer for WebSphere Software (RAD) . . . . . | 48 |
| Creación de un nuevo proyecto para una aplicación . . . . .                                                                                                      | 48 |
| Adición de un proyecto existente . . . . .                                                                                                                       | 49 |
| Adición de varios proyectos . . . . .                                                                                                                            | 51 |
| Adición de un nuevo proyecto Arxan. . . . .                                                                                                                      | 53 |
| Adición de un nuevo proyecto ASP . . . . .                                                                                                                       | 53 |
| Adición de un nuevo proyecto C/C++ . . . . .                                                                                                                     | 55 |
| Adición de un nuevo proyecto COBOL . . . . .                                                                                                                     | 57 |
| Adición de un nuevo proyecto ColdFusion . . . . .                                                                                                                | 57 |
| Adición de un nuevo proyecto Java o JavaServer Page (JSP) . . . . .                                                                                              | 58 |
| Adición de un nuevo proyecto de JavaScript . . . . .                                                                                                             | 66 |
| Adición de un nuevo proyecto .NET Assembly . . . . .                                                                                                             | 66 |
| Adición de un nuevo proyecto basado en patrón . . . . .                                                                                                          | 67 |
| Adición de un nuevo proyecto Perl . . . . .                                                                                                                      | 68 |
| Configuración de proyectos PHP . . . . .                                                                                                                         | 69 |
| Adición de un nuevo proyecto PL/SQL . . . . .                                                                                                                    | 80 |
| Adición de un nuevo proyecto T-SQL . . . . .                                                                                                                     | 81 |
| Adición de un nuevo proyecto Visual Basic. . . . .                                                                                                               | 82 |
| Cómo copiar proyectos . . . . .                                                                                                                                  | 82 |
| Modificación de las propiedades del proyecto y de la aplicación . . . . .                                                                                        | 83 |
| Atributos globales . . . . .                                                                                                                                     | 83 |
| Atributos de aplicación . . . . .                                                                                                                                | 84 |
| Eliminación de aplicaciones y proyectos . . . . .                                                                                                                | 85 |
| Vista Explorador. . . . .                                                                                                                                        | 85 |

## Capítulo 3. Preferencias . . . . . 93

|                                                                                                                                                                 |     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Preferencias generales . . . . .                                                                                                                                | 93  |
| Preferencias de AppScan Enterprise Console . . . . .                                                                                                            | 96  |
| Preferencias del servidor de aplicaciones para la compilación de JavaServer Page . . . . .                                                                      | 97  |
| Tomcat . . . . .                                                                                                                                                | 97  |
| WebLogic 11 y 12 . . . . .                                                                                                                                      | 98  |
| WebSphere Application Server . . . . .                                                                                                                          | 98  |
| Definición de variables . . . . .                                                                                                                               | 99  |
| Habilitación del seguimiento de defectos con preferencias . . . . .                                                                                             | 100 |
| Preferencias de Rational ClearQuest . . . . .                                                                                                                   | 100 |
| Preferencias de Quality Center . . . . .                                                                                                                        | 101 |
| Preferencias de Rational Team Concert . . . . .                                                                                                                 | 103 |
| Preferencias de Team Foundation Server . . . . .                                                                                                                | 104 |
| Importadores del espacio de trabajo de Eclipse: configuración de preferencias de Eclipse o Rational Application Developer for WebSphere Software (RAD). . . . . | 105 |
| Correo electrónico . . . . .                                                                                                                                    | 106 |
| Java y JavaServer Pages . . . . .                                                                                                                               | 106 |
| Artículos de la base de datos de conocimientos . . . . .                                                                                                        | 107 |
| Extensiones de archivo de proyecto . . . . .                                                                                                                    | 107 |

## Capítulo 4. Escaneo de código fuente y gestión de asesoramientos . . . . 109

|                                                                                                                                        |     |
|----------------------------------------------------------------------------------------------------------------------------------------|-----|
| Escaneo de código fuente . . . . .                                                                                                     | 109 |
| Escaneo de todas las aplicaciones. . . . .                                                                                             | 110 |
| Escaneo de una o varias aplicaciones . . . . .                                                                                         | 110 |
| Escaneo de uno o varios proyectos . . . . .                                                                                            | 110 |
| Escaneo de uno o varios archivos. . . . .                                                                                              | 111 |
| Volver a escanear código. . . . .                                                                                                      | 111 |
| Consideraciones de escaneo. . . . .                                                                                                    | 111 |
| Gestión de las configuraciones de escaneo. . . . .                                                                                     | 113 |
| Análisis incremental para Java. . . . .                                                                                                | 122 |
| Exclusión de un archivo de un escaneo. . . . .                                                                                         | 124 |
| Cancelar o detener un escaneo . . . . .                                                                                                | 125 |
| Requisito previo de componentes de AppScan Source for Analysis y AppScan Source for Development (plugin de Eclipse) en Linux . . . . . | 125 |
| Gestión de Mis asesoramientos . . . . .                                                                                                | 126 |
| Envío de asesoramientos de AppScan Source a la nube para su análisis. . . . .                                                          | 127 |
| Publicación de asesoramientos. . . . .                                                                                                 | 132 |
| Registro de aplicaciones y proyectos para publicar en AppScan Source . . . . .                                                         | 132 |
| Publicación de asesoramientos en AppScan Source. . . . .                                                                               | 133 |
| Publicación de asesoramientos en AppScan Enterprise Console . . . . .                                                                  | 135 |
| Guardar asesoramientos . . . . .                                                                                                       | 139 |
| Guardar asesoramientos automáticamente. . . . .                                                                                        | 140 |
| Eliminación de asesoramientos de Mis asesoramientos . . . . .                                                                          | 140 |
| Definición de variables . . . . .                                                                                                      | 141 |
| Definición de variables cuando se publican y se guardan . . . . .                                                                      | 142 |
| Ejemplo: definición de variables . . . . .                                                                                             | 142 |

## Capítulo 5. Selección y análisis . . . . 145

|                                                                                |     |
|--------------------------------------------------------------------------------|-----|
| Visualización de resultados. . . . .                                           | 146 |
| El proceso de selección de AppScan Source . . . . .                            | 148 |
| Selección de ejemplo . . . . .                                                 | 149 |
| Selección con filtros . . . . .                                                | 151 |
| Utilización de filtros predefinidos de AppScan Source. . . . .                 | 156 |
| Creación y gestión de filtros . . . . .                                        | 161 |
| Aplicación de filtros . . . . .                                                | 168 |
| Selección con exclusiones . . . . .                                            | 169 |
| El ámbito de las exclusiones . . . . .                                         | 169 |
| Especificación de exclusiones . . . . .                                        | 170 |
| Marcar resultados como exclusiones en una tabla de resultados . . . . .        | 170 |
| Volver a incluir resultados que se han marcado como exclusiones . . . . .      | 171 |
| Ejemplo: Especificación de exclusiones de filtro . . . . .                     | 171 |
| Especificación de exclusiones de paquetes desde la vista Propiedades . . . . . | 172 |
| Selección con paquetes . . . . .                                               | 172 |
| Creación de paquetes. . . . .                                                  | 173 |
| Adición de resultados a paquetes existentes . . . . .                          | 174 |
| Visualización de resultados en paquetes . . . . .                              | 174 |
| Guardado de paquetes en un archivo . . . . .                                   | 175 |

|                                                                                                                           |     |
|---------------------------------------------------------------------------------------------------------------------------|-----|
| Envío de paquetes para el seguimiento de defectos y por correo electrónico . . . . .                                      | 176 |
| Adición de notas a paquetes . . . . .                                                                                     | 176 |
| Modificar resultados . . . . .                                                                                            | 176 |
| Realizar modificaciones desde una tabla de resultados . . . . .                                                           | 177 |
| Modificación de resultados en la vista Detalle de resultado. . . . .                                                      | 178 |
| Eliminación de modificaciones de resultados . . . . .                                                                     | 180 |
| Comparación de resultados. . . . .                                                                                        | 182 |
| Comparación de dos asesoramientos en la vista Diferencia entre asesoramientos . . . . .                                   | 182 |
| Comparación de dos asesoramientos en la barra del menú principal . . . . .                                                | 182 |
| Búsqueda de diferencias entre asesoramientos en la vista Mis asesoramientos o en vista Asesoramientos publicados. . . . . | 182 |
| Resultados personalizados . . . . .                                                                                       | 183 |
| Creación de un resultado personalizado en la vista Propiedades . . . . .                                                  | 184 |
| Crear resultados personalizados en una vista de resultados . . . . .                                                      | 185 |
| Crear resultados personalizados en el editor de código fuente . . . . .                                                   | 185 |
| Resolución de problemas de seguridad y visualización de la asistencia de remediación. . . . .                             | 186 |
| Análisis del código fuente en un editor. . . . .                                                                          | 187 |
| Anotaciones y atributos soportados . . . . .                                                                              | 187 |

## Capítulo 6. Rastreo de AppScan Source . . . . . 191

|                                                                                |     |
|--------------------------------------------------------------------------------|-----|
| Resultados de escaneo del rastreo de AppScan Source. . . . .                   | 192 |
| Validación y codificación . . . . .                                            | 192 |
| Búsqueda de rastreos de AppScan Source . . . . .                               | 193 |
| Rastreo de entrada/salida . . . . .                                            | 193 |
| Utilización de la vista Rastreo . . . . .                                      | 194 |
| Pilas de entrada/salida en la vista Rastreo . . . . .                          | 194 |
| Análisis del código fuente en un editor. . . . .                               | 197 |
| Ámbito de la validación y codificación . . . . .                               | 198 |
| Creación de reglas personalizadas desde un rastreo de AppScan Source . . . . . | 199 |
| Ejemplos de código para el rastreo . . . . .                                   | 201 |
| Ejemplo 1: desde origen a receptor . . . . .                                   | 201 |
| Ejemplo 2: modificación entre origen y receptor . . . . .                      | 203 |
| Ejemplo 3: distintos archivos de origen y de recepción. . . . .                | 208 |
| Ejemplo 4: validación en profundidad . . . . .                                 | 209 |

## Capítulo 7. AppScan Source for Analysis y seguimiento de defectos. . 211

|                                                                          |     |
|--------------------------------------------------------------------------|-----|
| Habilitación del seguimiento de defectos con preferencias . . . . .      | 211 |
| Preferencias de Rational ClearQuest . . . . .                            | 211 |
| Preferencias de Quality Center . . . . .                                 | 212 |
| Preferencias de Rational Team Concert . . . . .                          | 214 |
| Preferencias de Team Foundation Server . . . . .                         | 215 |
| Integración de HP Quality Center y AppScan Source for Analysis . . . . . | 216 |
| Envío de resultados a Quality Center . . . . .                           | 216 |

|                                                                                                                   |     |
|-------------------------------------------------------------------------------------------------------------------|-----|
| Seguimiento de los resultados enviados a Quality Center . . . . .                                                 | 216 |
| Información de resultados de AppScan Source en Quality Center . . . . .                                           | 217 |
| Integración de Rational ClearQuest y AppScan Source for Analysis . . . . .                                        | 217 |
| Envío de resultados a Rational ClearQuest . . . . .                                                               | 217 |
| Envío de defectos a Rational ClearQuest . . . . .                                                                 | 218 |
| Integración de Rational Team Concert y AppScan Source for Analysis . . . . .                                      | 218 |
| Envío de defectos a Rational Team Concert . . . . .                                                               | 219 |
| Certificados SSL de Rational Team Concert . . . . .                                                               | 219 |
| Integración de Microsoft Team Foundation Server y AppScan Source for Analysis . . . . .                           | 220 |
| Envío de defectos a Microsoft Team Foundation Server . . . . .                                                    | 220 |
| Cómo trabajar con defectos enviados . . . . .                                                                     | 221 |
| Envío de paquetes para el seguimiento de defectos y por correo electrónico . . . . .                              | 221 |
| Seguimiento de defectos a través de correo electrónico (enviando los resultados por correo electrónico) . . . . . | 222 |

## **Capítulo 8. Informes de resultados e informes de auditoría . . . . . 223**

|                                                                                         |     |
|-----------------------------------------------------------------------------------------|-----|
| Crear informes de resultados . . . . .                                                  | 223 |
| Informes de AppScan Source . . . . .                                                    | 225 |
| Creación de un informe personalizado de AppScan Source . . . . .                        | 226 |
| Informe de CWE/SANS Top 25 2011 . . . . .                                               | 227 |
| Informe DISA Application Security and Development STIG V3R10 . . . . .                  | 228 |
| Informe Web Application Security Project (OWASP) Top 10 2013 . . . . .                  | 228 |
| Informe Web Application Security Project (OWASP) Mobile Top 10. . . . .                 | 228 |
| Informe de Payment Card Industry Data Security Standard (PCI DSS) Versión 3.2 . . . . . | 228 |
| Informe de Software Security Profile . . . . .                                          | 228 |

## **Capítulo 9. Creación de informes personalizados. . . . . 231**

|                                                                               |     |
|-------------------------------------------------------------------------------|-----|
| Editor de informe . . . . .                                                   | 231 |
| Separador Diseño de informe . . . . .                                         | 232 |
| Separador Categorías. . . . .                                                 | 233 |
| Separador Vista previa . . . . .                                              | 235 |
| Generación de informes personalizados . . . . .                               | 235 |
| Diseño de un informe a partir de un informe personalizado existente . . . . . | 236 |
| Inclusión de categorías en el informe . . . . .                               | 236 |
| Vista previa del informe. . . . .                                             | 237 |
| Cómo guardar la plantilla del informe . . . . .                               | 237 |

## **Capítulo 10. Personalización de la base de datos de vulnerabilidad y de las reglas de patrón . . . . . 239**

|                                                                                      |     |
|--------------------------------------------------------------------------------------|-----|
| Ampliación de la Base de datos de conocimientos de AppScan Source Security . . . . . | 239 |
| Creación de reglas personalizadas . . . . .                                          | 240 |

|                                                                                                |     |
|------------------------------------------------------------------------------------------------|-----|
| Utilización del Asistente de reglas personalizadas . . . . .                                   | 240 |
| Atributos de reglas de probabilidad. . . . .                                                   | 246 |
| Personalización del rastreo de entrada/salida a través del rastreo de AppScan Source . . . . . | 247 |
| Personalización con reglas basadas en patrón. . . . .                                          | 247 |
| Conjuntos de reglas de patrón. . . . .                                                         | 248 |
| Reglas de patrón . . . . .                                                                     | 250 |
| Aplicación de reglas de patrón y de conjuntos de reglas . . . . .                              | 254 |

## **Capítulo 11. Ampliación de la infraestructura de importación del servidor de aplicaciones . . . . . 267**

## **Capítulo 12. Ejemplo de AppScan Source for Analysis. . . . . 273**

## **Capítulo 13. El entorno de trabajo de AppScan Source for Analysis . . . . . 275**

|                                                                |     |
|----------------------------------------------------------------|-----|
| El espacio de trabajo de AppScan Source for Analysis . . . . . | 275 |
| Menú principal. . . . .                                        | 277 |
| Menú Archivo . . . . .                                         | 277 |
| Menú Editar. . . . .                                           | 281 |
| Menú Escanear. . . . .                                         | 282 |
| Menú Herramientas . . . . .                                    | 283 |
| Menú Administración . . . . .                                  | 284 |
| Menú Vista . . . . .                                           | 284 |
| Menú Perspectiva . . . . .                                     | 284 |
| Menú Ayuda . . . . .                                           | 285 |
| Barras de herramientas . . . . .                               | 286 |
| Ayuda flotante . . . . .                                       | 286 |
| Barra de estado. . . . .                                       | 286 |

## **Capítulo 14. Vistas . . . . . 289**

|                                                             |     |
|-------------------------------------------------------------|-----|
| Vistas de configuración . . . . .                           | 289 |
| Vista Reglas personalizadas . . . . .                       | 289 |
| Vista Explorador . . . . .                                  | 289 |
| Vista Biblioteca de reglas de patrón . . . . .              | 295 |
| Vista Propiedades . . . . .                                 | 296 |
| Vista Configuración del escaneo . . . . .                   | 305 |
| Editor de informe . . . . .                                 | 308 |
| Vistas que ayudan con la salida de escaneo . . . . .        | 312 |
| Vista Consola . . . . .                                     | 312 |
| Vista Métricas . . . . .                                    | 313 |
| Vista Mis asesoramientos . . . . .                          | 313 |
| Vista Asesoramientos publicados . . . . .                   | 314 |
| Vistas que ayudan con la selección . . . . .                | 315 |
| Vista Diferencia entre asesoramientos . . . . .             | 315 |
| Vista Resultados personalizados . . . . .                   | 316 |
| Vistas con resultados . . . . .                             | 316 |
| Vista Entradas y salidas . . . . .                          | 325 |
| Vistas que permiten investigar un resultado único . . . . . | 326 |
| Vista Detalle de resultado . . . . .                        | 326 |
| Vista Asistencia de remediación . . . . .                   | 329 |
| Vista Rastreo . . . . .                                     | 329 |
| Vistas que permiten trabajar con asesoramientos . . . . .   | 331 |
| Vista Resumen de asesoramiento . . . . .                    | 331 |

|                                          |     |
|------------------------------------------|-----|
| Vista Editor de filtros . . . . .        | 332 |
| Vista Matriz de vulnerabilidad . . . . . | 332 |
| Vista Paquetes . . . . .                 | 334 |
| Vista Paquetes . . . . .                 | 334 |

## **Capítulo 15. Soporte a CWE . . . . . 339**

### **Glosario . . . . . 341**

|             |     |
|-------------|-----|
| A . . . . . | 341 |
| C . . . . . | 341 |
| D . . . . . | 341 |
| E . . . . . | 342 |

|             |     |
|-------------|-----|
| F . . . . . | 342 |
| G . . . . . | 342 |
| M . . . . . | 342 |
| P . . . . . | 342 |
| R . . . . . | 343 |
| S . . . . . | 343 |
| X . . . . . | 343 |

### **Avisos . . . . . 345**

### **Índice. . . . . 349**



---

# Capítulo 1. Introducción a AppScan Source for Analysis

En esta sección se describe cómo se adapta AppScan Source for Analysis a la solución AppScan Source total y ofrece una base para comprender el flujo de trabajo de seguridad del software.

---

## Introducción a IBM Security AppScan Source

IBM® Security AppScan Source ofrece un valor máximo a cada usuario en la organización que desempeña un papel importante en la seguridad de software. Tanto como si es un analista de control de calidad o seguridad, desarrollador o ejecutivo, los productos de AppScan Source ofrecen la funcionalidad, la flexibilidad y la potencia que necesita para su escritorio.

El conjunto de productos incluye:

- **AppScan Source for Analysis:** Entorno de trabajo para configurar aplicaciones y proyectos, escanear código, analizar, seleccionar y tomar medidas en la prioridad de vulnerabilidades.
- **AppScan Source for Automation:** Le permite automatizar los aspectos clave del flujo de trabajo de AppScan Source e integrar seguridad con entornos de compilación durante el ciclo de vida del desarrollo del software.
- **AppScan Source for Development:** Los plugins de Developer integran muchas características de AppScan Source for Analysis en Microsoft Visual Studio, el entorno de trabajo de Eclipse y Rational Application Developer for WebSphere Software (RAD). Esto permite a los desarrolladores de software encontrar las vulnerabilidades y actuar en relación a las mismas, durante el proceso de desarrollo. El plugin de Eclipse permite escanear código fuente en busca de vulnerabilidades de seguridad y puede escanear proyectos de IBM MobileFirst Platform con los plugins de Eclipse.

Para ampliar el valor de AppScan Source en la organización, los productos incluyen estos componentes:

- **Base de datos de conocimientos de AppScan Source Security:** Inteligencia en contexto para cada vulnerabilidad, ofreciendo descripciones precisas acerca de la causa raíz, la gravedad de riesgo y los consejos de solución procesables.
- **AppScan Enterprise Server:** La mayoría de los componentes y productos de AppScan Source se deben comunicar con una instancia de AppScan Enterprise Server. Sin esto, podrá utilizar AppScan Source for Development en modo local, pero algunas características como, por ejemplo, las reglas personalizadas, las configuraciones de escaneo y los filtros compartidos no estarán disponibles.

El servidor ofrece funciones de gestión de usuario centralizadas y un mecanismo para compartir asesoramientos a través de la base de datos de AppScan Source. El servidor incluye un componente de Enterprise Console opcional. Si el administrador instala este componente, puede publicar asesoramientos en él a partir de AppScan Source for Analysis, AppScan Source for Automation, y la interfaz de línea de mandatos (CLI) de AppScan Source. Enterprise Console ofrece una variedad de herramientas para trabajar con asesoramientos, como característica de informes, gestión de problemas, análisis de tendencias y paneles de control.

**Importante:** Para algunas versiones de AppScan Source y AppScan Enterprise, el nivel de versión y release de los dos productos deben coincidir para poder conectarse desde AppScan Source a AppScan Enterprise Server. Consulte <http://www.ibm.com/support/docview.wss?uid=swg21975211> para conocer qué versiones de AppScan Source y AppScan Enterprise son compatibles.

**Nota:**

- No se da soporte a AppScan Enterprise Server en macOS.
- Si posee una licencia de servidor básica, es posible que al servidor puedan acceder un máximo de 10 conexiones desde productos AppScan. Con una licencia de servidor premium, se permiten conexiones ilimitadas.

**Importante:** Cuando se escanea, los clientes de AppScan Enterprise Server y AppScan Source (excepto AppScan Source for Development) precisan una conexión directa a la base de datos de AppScan Source (tanto solidDB como Oracle).

Esta oferta de Software no utiliza cookies u otras tecnologías para recopilar personalmente información identificable.

## Traducciones

Las interfaces de usuario de AppScan Source están disponibles en los siguientes idiomas:

- Inglés
- Portugués (Brasil)
- Chino (simplificado)
- Chino (tradicional)
- Alemán
- Español
- Francés
- Italiano
- Japonés
- Coreano
- Ruso

## Cumplimiento de las regulaciones del Gobierno de los Estados Unidos

Cumplimiento con las regulaciones de tecnología de la información y seguridad del Gobierno de los Estados Unidos para eliminar los impedimentos y barreras a las ventas. También proporciona la prueba a los potenciales clientes de que IBM está trabajando para hacer que sus productos sean los más seguros del sector. En este tema se enumeran los estándares y directrices que AppScan Source soporta.

- “Protocolo de Internet versión 6 (IPv6)” en la página 3
- “FIPS (Federal Information Processing Standard)” en la página 3
- “NIST SP 800-131A (National Institute of Standards and Technology Special Publication 800-131A)” en la página 3
- “Máquinas Windows 7 configuradas para utilizar la especificación USGCB (United States Government Configuration Baseline)” en la página 4

## Protocolo de Internet versión 6 (IPv6)

AppScan Source está habilitado para IPv6, con estas excepciones:

- No se da soporte a la entrada de direcciones numéricas IPv6 y en su lugar se debe especificar un nombre de host. Introducir direcciones numéricas IPv4 está admitido.
- No se da soporte a IPv6 al conectarse a Rational Team Concert.

## FIPS (Federal Information Processing Standard)

AppScan Source da soporte a FIPS SP 140-2, utilizando algoritmos aprobados y un módulo criptográfico validado FIPS 140-2 en las plataformas Windows y Linux a las que AppScan Source da soporte. En las plataformas macOS a las que AppScan Source da soporte, se necesitan pasos manuales para trabajar en la modalidad FIPS 140-2.

Obtenga información general sobre el cumplimiento FIPS por parte de AppScan Source y de cómo habilitar en inhabilitar la modalidad FIPS 140-2 en AppScan Source, consultando estas notas técnicas:

- Operating AppScan Source version 8.7 or later in FIPS 140-2 mode on macOS
- How to enable/disable/verify FIPS 140-2 mode in AppScan Source (Linux and Windows)
- Background information about AppScan Source version 8.7 or later FIPS 140-2 support

## NIST SP 800-131A (National Institute of Standards and Technology Special Publication 800-131A)

Las directrices NIST SP 800-131A proporcionan una guía en la gestión de claves criptográficas. Estas directrices incluyen:

- Procedimientos de gestión de claves.
- Utilización de algoritmos criptográficos.
- Utilización de algoritmos y sus fortalezas mínimas.
- Longitudes de claves para comunicaciones seguras.

Las agencias gubernamentales y las instituciones financieras utilizan las directrices NIST SP 800-131A para asegurarse de que los productos se ajustan a los requisitos de seguridad especificados.

Sólo se da soporte a NIST SP 800-131A cuando AppScan Source está funcionando en la modalidad FIPS 140-2. Para obtener más información sobre cómo habilitar e inhabilitar la modalidad FIPS 140-2 en AppScan Source, consulte “FIPS (Federal Information Processing Standard)”.

**Importante:** Si la instancia de AppScan Enterprise Server a la que se conectará está habilitada para el cumplimiento del estándar NIST 800-131a, debe establecer AppScan Source para forzar Transport Layer Security V1.2. Si no se fuerza Transport Layer Security V1.2, las conexiones al servidor fallarán.

- Si la base de datos de AppScan Source **no** está instalada (por ejemplo, sólo está instalando los componentes de cliente), puede forzar Transport Layer Security V1.2 modificando `<dir_datos>\config\ounce.ozsettings` (donde `<data_dir>` es

la ubicación de los datos de programa AppScan Source, como se describe en “Instalación y ubicaciones de archivo de datos de usuario” en la página 335)). En este archivo, localice este valor:

```
<Setting
  name="tls_protocol_version"
  read_only="false"
  default_value="0"
  value="0"
  description="Minor Version of the TLS Connection Protocol"
  type="text"
  display_name="TLS Protocol Version"
  display_name_id=""
  available_values="0:1:2"
  hidden="false"
  force_upgrade="false"
/>
```

En este valor, cambie value="0" por value="2" y, a continuación, guarde el archivo.

- Si está instalando la base de datos de AppScan Source, Transport Layer Security V1.2 se fuerza en la herramienta de configuración de la base de datos de IBM Security AppScan Enterprise Server después de instalar AppScan Source y Enterprise Server.

## **Máquinas Windows 7 configuradas para utilizar la especificación USGCB (United States Government Configuration Baseline)**

AppScan Source da soporte a aplicaciones en Windows 7 configuradas con la especificación USGCB.

**Nota:** En máquinas configuradas con la especificación USGCB, AppScan Source no da soporte a la integración del sistema de rastreo de defectos con HP Quality Center o Rational ClearQuest.

---

## **Novedades de AppScan Source**

Explore estas nuevas características que se han añadido a AppScan Source y anote las características y prestaciones que han caído en desuso en este release.

- “Novedades en AppScan Source Versión 9.0.3.7”
- “Novedades en AppScan Source Versión 9.0.3.6” en la página 5
- “Novedades en AppScan Source Versión 9.0.3.5” en la página 5
- “Novedades en AppScan Source Versión 9.0.3.4” en la página 6
- “Novedades de AppScan Source Versión 9.0.3.3” en la página 8
- “Novedades en AppScan Source Versión 9.0.3.2” en la página 10
- “Novedades de AppScan Source Versión 9.0.3.1” en la página 10
- “Novedades de AppScan Source Versión 9.0.3” en la página 11

### **Novedades en AppScan Source Versión 9.0.3.7**

- “Nuevo soporte de escaneo mejorado ”
- “Prestaciones y características que ya no están soportadas en AppScan Source Versión 9.0.3.7” en la página 5

#### **Nuevo soporte de escaneo mejorado**

- Red Hat Enterprise Linux (RHEL) Versión 7.3 es ahora un sistema operativos soportado.

- Ahora se da soporte a la aplicación de Plugin AppScan Source for Development Visual Studio en Visual Studio 2015.

### **Prestaciones y características que ya no están soportadas en AppScan Source Versión 9.0.3.7**

A partir de AppScan Source Versión 9.0.3.7:

- OS X Versión 10.10 ya no es un sistema operativo soportado.
- La versión 6.3 de Xcode ya no está soportada. Ya no está soportado escanear proyectos Objective-C con esta versión de Xcode.
- Las versiones 5 y 6 de Tomcat ya no están soportadas.

### **Novedades en AppScan Source Versión 9.0.3.6**

- “Nuevo soporte de escaneo mejorado ”
- “Prestaciones y características que ya no están soportadas en AppScan Source Versión 9.0.3.6”

#### **Nuevo soporte de escaneo mejorado**

- Xcode 8.1 y 8.2 para Objective-C (sólo para aplicaciones iOS) son ahora compiladores soportados en macOS. El soporte para estas versiones de Xcode es retroactivo para AppScan Source Versión 9.0.3.5.

### **Prestaciones y características que ya no están soportadas en AppScan Source Versión 9.0.3.6**

A partir de AppScan Source Versión 9.0.3.6:

- Red Hat Enterprise Linux Versión 5 ya no es un sistema operativo soportado.
- Oracle WebLogic Server versiones 8, 9 y 10 dejan de ser compiladores soportados.

### **Novedades en AppScan Source Versión 9.0.3.5**

- “Nuevo soporte de escaneo mejorado ”
- “Soporte de escaneo incremental para bytecode y archivos de origen Java que permite volver a escanear de forma más eficiente y rápida”

#### **Nuevo soporte de escaneo mejorado**

- Ahora se da soporte al sistema operativo a macOS Versión 10.12. El soporte para macOS Versión 10.12 es retroactivo a AppScan Source Versión 9.0.3.4.
- Xcode 8.0, 8.1 y 8.2 para Objective-C (únicamente para aplicaciones iOS) son ahora compiladores soportados en macOS.

#### **Soporte de escaneo incremental para bytecode y archivos de origen Java que permite volver a escanear de forma más eficiente y rápida**

A partir de la versión 9.0.3.5, se puede habilitar el soporte al escaneo incremental de Java en Windows y Linux. Cuando se habilita el escaneo incremental, AppScan Source coloca en la caché los datos de análisis. Cuando se vuelve a escanear un proyecto o aplicación, AppScan Source utiliza estos datos para determinar los cambios de código de forma que únicamente se analizan de nuevo las partes del código afectadas por los cambios. El resultado es un análisis completo del código, pero en una fracción del tiempo.

Se da soporte a esta característica con IBM Security AppScan Source for Analysis, el Plugin AppScan Source for Development Eclipse , IBM Security AppScan Source for Automation, o la interfaz de línea de mandatos (CLI) de IBM Security AppScan Source.

## **Novedades en AppScan Source Versión 9.0.3.4**

- “Nuevo soporte de escaneo mejorado ”
- “Ahora se da soporte a la publicación de asesoramientos para AppScan Enterprise Console al realizar la autenticación con Common Access Card (CAC)”
- “Soporte al informe de Payment Card Industry Data Security Standard (PCI DSS) Versión 3.2”
- “Documentación del producto AppScan Source for Analysis”
- “Posibilidad de utilizar configuraciones de escaneo en AppScan Source for Analysis para eliminar resultados de cualquier filtro de exclusión” en la página 7
- “Mejoras en el manejo de bibliotecas al escanear archivos WAR y EAR en AppScan Source for Automation y en la interfaz de línea de mandatos (CLI) de AppScan Source” en la página 8
- “Envío de asesoramientos de AppScan Source a la nube para su análisis” en la página 8
- “Prestaciones y características que ya no están soportadas en AppScan Source Versión 9.0.3.4” en la página 8

### **Nuevo soporte de escaneo mejorado**

Ahora es posible escanear PHP versión 7.0 en Windows y Linux en IBM Security AppScan Source for Analysis, IBM Security AppScan Source for Automation y en la interfaz de línea de mandatos (CLI) de IBM Security AppScan Source.

### **Ahora se da soporte a la publicación de asesoramientos para AppScan Enterprise Console al realizar la autenticación con Common Access Card (CAC)**

Si está utilizando la autenticación con CAC para conectarse a AppScan Enterprise Server, ahora puede publicar los asesoramientos en AppScan Enterprise Console desde la interfaz de usuario de AppScan Source, la interfaz de línea de mandatos (CLI) de AppScan Source y AppScan Source for Automation.

### **Soporte al informe de Payment Card Industry Data Security Standard (PCI DSS) Versión 3.2**

AppScan Source ahora da soporte al informe Payment Card Industry Data Security Standard (PCI DSS) Versión 3.2.

### **Documentación del producto AppScan Source for Analysis**

A partir de la versión 9.0.3.4, cuando utiliza el elemento de menú **Ayuda > Contenido de ayuda** en AppScan Source for Analysis, se abre la ayuda en línea para AppScan Source en el IBM Knowledge Center (para la versión 9.0.3.4, la ayuda en línea abre la documentación de IBM Security AppScan SourceV9.0.3.4). De forma parecida, cuando sigue los enlaces desde la vista Bienvenido a AppScan Source for Analysis, se abren en el IBM Knowledge Center.

AppScan Source for Analysis también ofrece ayuda sensible al contexto en muchas vistas, páginas de preferencias y recuadros de diálogo. El atajo del teclado para la

ayuda sensible al contexto es F1 en Windows, Mayúsculas+F1 en Linux y Mandato+F1 en macOS. Esta ayuda sensible al contexto también se abre en AppScan Source en IBM Knowledge Center a partir de la versión 9.0.3.4.

Si está utilizando el producto sin una conexión a internet, ya ayuda está disponible localmente de la siguiente manera:

- El archivo Readme y las Notas del release de IBM Security AppScan Source están disponibles en el archivo `readme.html` que está ubicado el directorio de instalación de AppScan Source.
- Estas guías de usuario en formato PDF están en el directorio `doc/<idioma>` o `doc\<idioma>` del directorio de instalación de AppScan Source (donde `<idioma>` es el idioma de su instalación de AppScan Source):
  - Únicamente Windows y Linux: *IBM Security AppScan Source for Analysis Guía del usuario* (`Security_AppScan_Source_Analysis.pdf`)
  - Únicamente Windows y Linux: *IBM Security AppScan Source Utilities Guía del usuario* (`Security_AppScan_Source_Uutilities.pdf`)
  - Únicamente macOS: *IBM Security AppScan Source for Analysis Guía del usuario para macOS* (`Security_AppScan_Source_Analysis_OSX.pdf`)
  - Únicamente macOS: *IBM Security AppScan Source Utilities Guía del usuario para macOS* (`Security_AppScan_Source_Uutilities_OSX.pdf`)
  - *IBM Security AppScan Source Guía de instalación y administración* (`Security_AppScan_Source_Installation_and_Administration.pdf`)

Debe tener Adobe Acrobat Reader para leer estos archivos. Si no tiene una copia de Acrobat Reader, puede descargarla de <http://www.adobe.com/>.

- La documentación Javadoc para algunas de las características de AppScan Source for Analysis se encuentra ubicada en el directorio `doc/Javadoc` o `doc\Javadoc` del directorio de instalación de AppScan Source. A partir de la versión 9.0.3.4, hay disponible Javadoc para estas características:
  - Javadoc para los métodos y las clases de API de infraestructura de importación de servidor de aplicaciones en `doc/Javadoc/appserverimporter` o `doc\Javadoc\appserverimporter`.
  - Javadoc para los métodos y las clases de API de infraestructuras para infraestructuras en `doc/Javadoc/frameworks` o `doc\Javadoc\frameworks`.

En estas carpetas, abra el archivo `index.html`.

## **Posibilidad de utilizar configuraciones de escaneo en AppScan Source for Analysis para eliminar resultados de cualquier filtro de exclusión**

Los filtros de exclusión contienen reglas para qué tipos de vulnerabilidad, interfaces de programación de aplicaciones (API), archivos, directorios, proyectos o reglas de rastreo se eliminen de los resultados. Si incluye varios filtros de exclusión en una configuración de escaneo, es posible que entren en conflicto entre sí y afecten a los resultados. Por ejemplo, dados estos dos filtros:

- El Filtro 1 elimina todos los resultados del tipo de vulnerabilidad `Validation.EncodingRequired`. No está invertido de forma que estos resultados se excluirán del asesoramiento.
- El Filtro 2 elimina todos los resultados del tipo de vulnerabilidad `Validation.Required`. No está invertido de forma que estos resultados se excluirán del asesoramiento.

Si ambos filtros se aplican utilizando una configuración de escaneo, de forma predeterminada se descartarán entre sí. El Filtro 1 excluirá los resultados `Validation.EncodingRequired`, pero incluirá los resultados `Validation.Required`. El Filtro 2 excluirá los resultados `Validation.Required`, pero incluirá los resultados `Validation.EncodingRequired`. El resultado final será que se incluirán los resultados `Validation.EncodingRequired` y `Validation.Required`.

A partir de la versión 9.0.3.4, puede eliminar resultados de *cualquier* filtro de exclusión especificado seleccionando **Coincidencia de cualquier filtro de exclusión no invertido** al crear una configuración de escaneo. Este recuadro de selección se encuentra en la sección **Información de filtros** del separador **General** de la vista Configuración de escaneo. Con el ejemplo anterior, si se selecciona este recuadro de selección, todos los resultados `Validation.EncodingRequired` y `Validation.Required` se excluirán del asesoramiento.

## **Mejoras en el manejo de bibliotecas al escanear archivos WAR y EAR en AppScan Source for Automation y en la interfaz de línea de mandatos (CLI) de AppScan Source**

Al escanear archivos WAR, ahora hay disponibles estas opciones:

- `-include_all_lib_jars`: Este valor sirve para incluir durante el escaneo todas las biblioteca en el archivo WAR.
- `-include_lib_jars`: Este valor sirve para especificar las bibliotecas en el archivo WAR que desea incluir durante el escaneo.

Al importar un archivo EAR, se crea automáticamente un proyecto para almacenar las bibliotecas compartidas. Si no hay bibliotecas compartidas, se creará el proyecto pero estará vacío. El valor `-no_ear_project` está ahora disponible, y cuando se utiliza, no se creará un proyecto para el archivo EAR.

## **Envío de asesoramientos de AppScan Source a la nube para su análisis**

Si posee una suscripción a IBM Application Security on Cloud en IBM Cloud Marketplace o a Application Security on Cloud for Bluemix, puede enviar asesoramientos de AppScan Source para su análisis en la nube. Se da soporte a los asesoramientos de AppScan Source versiones 9.0 o superiores. El número de escaneos que se pueden enviar dependen de su suscripción de Application Security on Cloud. Consulte el apartado [http://www.ibm.com/support/knowledgecenter/SSYJF1.0.0/ApplicationSecurityonCloud/src\\_managing\\_assessments\\_cloud.html](http://www.ibm.com/support/knowledgecenter/SSYJF1.0.0/ApplicationSecurityonCloud/src_managing_assessments_cloud.html) para obtener más información.

## **Prestaciones y características que ya no están soportadas en AppScan Source Versión 9.0.3.4**

A partir de AppScan Source Versión 9.0.3.4:

- OS X Versión 10.9 ya no es un sistema operativo soportado.
- Ya no se da soporte a Xcode versiones 5.x, 6.0 y 6.2. Ya no se da soporte al escaneo de proyectos de Objective-C con estas versiones de Xcode.
- El soporte para el escaneo de PHP versiones 5.3 y 5.4 está en desuso.

## **Novedades de AppScan Source Versión 9.0.3.3**

- “Soporte de soluciones de integración y nuevas plataformas ” en la página 9
- “Nuevo soporte de escaneo mejorado ” en la página 10



- “Nuevo nombre de archivo de instalación para Windows” en la página 10
- “Soporte a CAC (Common Access Card) en Windows” en la página 10
- “Soporte de informes de DISA Application Security and Development STIG V3R10 ” en la página 10

## Soporte de soluciones de integración y nuevas plataformas

A partir de AppScan Source Versión 9.0.3.3:

- Microsoft Windows 10 es ahora un sistema operativo soportado. Se incluyen las ediciones Windows 10 Education, Enterprise y Pro.

### Nota:

- En Windows 10, el instalador de AppScan Source (archivo AppScanSrc\_Installer.exe) se debe ejecutar en la modalidad de compatibilidad de Windows 7. En Windows 10, también se debe configurar el archivo AppScan\_Uninstaller.exe para que se ejecute en la modalidad de compatibilidad de Windows 7 antes de desinstalar AppScan Source. Este archivo se encuentra en <dir\_instalación>\Uninstall\_AppScan\ AppScan\_Uninstaller.exe (donde <dir\_instalación> es la ubicación de su instalación de AppScan Source, como se describe en “Instalación y ubicaciones de archivo de datos de usuario” en la página 335). Consulte <http://www.ibm.com/support/docview.wss?uid=swg21696098> para obtener más información.
- El soporte a Windows 10 se ve afectado por el problema descrito en <http://www.ibm.com/support/docview.wss?uid=swg21689814>.
- Si se está conectando a una instancia de AppScan Enterprise Server Versión 9.0.3.1 o superior, la base de datos de IBM Security AppScan Source se puede instalar en una base de datos Oracle 12c.

**Importante:** Si posee una instalación existente de AppScan Source que utilice la base de datos Oracle 11g, y desea actualizarla a Oracle 12c, debe actualizar AppScan Source antes de actualizar la base de datos de Oracle.

- Ahora se incluye a **Tomcat 8** en la instalación de AppScan Source.
- Ahora los archivos de proyectos y soluciones de Visual Studio 2015 se pueden escanear en AppScan Source for Analysis, AppScan Source for Automation y en la AppScan Source. Si tiene archivos .sln o .vcproj creados en Visual Studio 2015, es posible importar y escanear en Windows estos archivos utilizando AppScan Source for Analysis, AppScan Source for Automation o la AppScan Source.

### Importante:

- No se da soporte a la aplicación del Plugin AppScan Source for Development Visual Studio en Visual Studio 2015.
- Se da soporte a proyecto C++ gestionados. También se da soporte a los proyectos C++ no gestionados si se generan con un conjunto de herramientas de plataforma (Platform Toolset) desde Visual Studio 2013 o anterior (Platform Toolset V120 o anterior).
- Xcode 7.3 for Objective-C (únicamente para aplicaciones iOS) es ahora un compilador soportado en macOS (el soporte para Xcode 7.3 se aplica de forma retroactiva a AppScan Source Versión 9.0.3.2).

## **Nuevo soporte de escaneo mejorado**

- Ahora es posible escanear PHP versiones 5.5 y 5.6 en Windows y Linux en IBM Security AppScan Source for Analysis, IBM Security AppScan Source for Automation, y la interfaz de línea de mandatos (CLI) de IBM Security AppScan Source.
- Ahora se da soporte a la utilización de AppScan Source para escanear anotaciones a nivel de método de Java™, @ValidatorMethod, @CallbackMethod y @SuppressSecurityTrace.

## **Nuevo nombre de archivo de instalación para Windows**

En Windows, el nombre del archivo de instalación a cambiado de setup.exe a AppScanSrc\_Installer.exe.

## **Soporte a CAC (Common Access Card) en Windows**

La Common Access Card (<http://www.cac.mil>) es el estándar de identificación para el personal de los servicios uniformados activos, de la reserva militar, de los empleados del Ministerio de Defensa y del personal contratado en los Estados Unidos. Se utiliza para permitir el acceso físico a edificios y espacios controlados y proporciona acceso a las redes y sistemas del Ministerio de Defensa (DoD). CAC se puede utilizar para acceder a sistemas y redes equipadas con diferentes lectores de tarjetas inteligentes. Cuando se inserta en el lector, el dispositivo solicita al usuario un PIN.

Si ejecuta AppScan Source en Windows y se conecta a una instancia de AppScan Enterprise Server Versión 9.0.3.1 iFix-001 o superior habilitado para autenticación con CAC (Common Access Card), AppScan Source ahora da soporte a la autenticación con CAC.

## **Soporte de informes de DISA Application Security and Development STIG V3R10**

AppScan Source ahora da soporte a los informes de Defense Information Systems Agency (DISA) Application Security y Development Security Technical Implementation Guide (STIG) V3R10.

## **Novedades en AppScan Source Versión 9.0.3.2**

### **Compatibilidad de versiones entre AppScan Source y AppScan Enterprise**

Algunas versiones de AppScan Source ya no necesitan que los niveles de versión y release de AppScan Source y AppScan Enterprise coincidan al conectarse a AppScan Enterprise Server o al publicar en AppScan Enterprise Console. Consulte <http://www.ibm.com/support/docview.wss?uid=swg21975211> para conocer qué versiones de AppScan Source y AppScan Enterprise son compatibles.

Este cambio es retroactivo para algunas versiones de AppScan Source, tal como se describe en <http://www.ibm.com/support/docview.wss?uid=swg21975211>.

## **Novedades de AppScan Source Versión 9.0.3.1**

- “Nuevo soporte de soluciones de integración ” en la página 11
- “Escaneo de archivos WAR y EAR en AppScan Source for Automation y en la interfaz de línea de mandatos (CLI) de AppScan Source” en la página 11

## Nuevo soporte de soluciones de integración

A partir de AppScan Source Versión 9.0.3.1:

- Se admite Tomcat 8 para la compilación de Java y JSP.

**Nota:** El soporte del sistema operativo depende del sistema operativo compatible con cada uno de los compiladores.

- Xcode 7.0, 7.1 y 7.2 for Objective-C (únicamente para aplicaciones iOS) son ahora compiladores soportados en macOS.

## Escaneo de archivos WAR y EAR en AppScan Source for Automation y en la interfaz de línea de mandatos (CLI) de AppScan Source

El mandato `openapplication (oa)` de la CLI ahora se puede utilizar para abrir archivos WAR y EAR. Además, estos archivos se pueden escanear en AppScan Source for Automation con el mandato `ScanApplication`.

## Novedades de AppScan Source Versión 9.0.3

- “Soporte de soluciones de integración y nuevas plataformas ”
- “Mejoras de configuración de escaneo” en la página 12
- “Los atributos de reglas nuevas le permiten identificar resultados de seguridad definitivos de alta gravedad de forma más precisa” en la página 12
- “La resolución automática de receptor perdido permite mejores resultados de escaneo” en la página 13
- “Nuevo soporte de escaneo mejorado ” en la página 13
- “Prestaciones y características que ya no están soportadas en AppScan Source Versión 9.0.3” en la página 14

## Soporte de soluciones de integración y nuevas plataformas

A partir de AppScan Source Versión 9.0.3, se da soporte a los siguientes sistemas operativos:

- Red Hat Enterprise Linux Versión 6 Actualizaciones 6 y 7
- OS X Versión 10.11. El soporte para OS X Versión 10.11 es retroactivo para AppScan Source Versión 9.0.2, con la limitación descrita en <http://www.ibm.com/support/docview.wss?uid=swg21968948> (esta limitación sólo afecta a AppScan Source Versión 9.0.2).

Además:

- Xcode 6.3 y 6.4 para Objective-C (sólo para aplicaciones de iOS) son ahora compiladores soportados en OS X (el soporte para Xcode 6.3 y 6.4 es retroactivo a AppScan Source Versión 9.0.2). Tenga en cuenta que existen algunas limitaciones para el soporte de Xcode 6.3 y 6.4. Consulte <http://www.ibm.com/support/docview.wss?uid=swg21962208> para obtener más detalles. Estas limitaciones no se aplican a AppScan Source Versión 9.0.3.1 y superiores.
- El Plugin AppScan Source for Development Eclipse ahora se integra con IBM MobileFirst Platform Foundation Versión 7.1. Ahora puede escanear proyectos, aplicaciones, entornos y archivos HTML de IBM MobileFirst Platform Versión 7.1 en productos AppScan Source.

- Se pueden escanear archivos de proyecto y espacios de trabajo de Rational Application Developer for WebSphere Software (RAD) Versión 9.1.1, y el AppScan Source for Development (plugin de Eclipse) se puede aplicar a RAD Versión 9.1.1.
- Los espacios de trabajo y archivos de proyectos de Eclipse Versión 4.5 (sólo Java y IBM MobileFirst Platform) se pueden escanear, y se puede aplicar AppScan Source for Development (plugin de Eclipse) a Eclipse Versión 4.5.
- Se admite IBM WebSphere Application Server Versión 8.5.5 para la compilación de Java y JSP.

**Nota:** El soporte del sistema operativo depende del sistema operativo compatible con cada uno de los compiladores.

## Mejoras de configuración de escaneo

La vista Configuración del escaneo se ha rediseñado y ahora ofrece estas características clave:

- La posibilidad de especificar filtros.
- Establecimiento del tipo de análisis a realizar durante un escaneo. Esto incluye el análisis de flujo corrupto y el análisis basado en patrón.

AppScan Source incluye ahora estas configuraciones de escaneo integradas: Escaneo de vista previa web, Escaneo rápido web, Escaneo equilibrado web y Escaneo profundo web

## Los atributos de reglas nuevas le permiten identificar resultados de seguridad definitivos de alta gravedad de forma más precisa

Este release de AppScan Source presenta los atributos `Attribute.Likelihood.High` y `Attribute.Likelihood.Low`. Estos atributos se han añadido a las reglas predefinidas y también se pueden utilizar al crear reglas personalizadas.

En AppScan Source, *probabilidad* representa la probabilidad o la oportunidad de que se pueda explotar un resultado de seguridad. AppScan Source toma la definición de probabilidad presente en [https://www.owasp.org/index.php/OWASP\\_Risk\\_Rating\\_Methodology#Step\\_2:\\_Factors\\_for\\_Estimating\\_Likelihood](https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology#Step_2:_Factors_for_Estimating_Likelihood), y la acota determinando la probabilidad en función de las propiedades de rastreo. Dado un conjunto de propiedades de rastreo (por ejemplo, nombre de API de origen, tipo de API de origen, tecnología de origen o mecanismo de origen), AppScan Source determinará la probabilidad de que un rastreo pueda o sea explotado mediante una vulnerabilidad específica en el futuro.

La probabilidad está unida al elemento de origen de un rastreo. Un origen es una entrada para el programa, como un archivo, una solicitud de servlet, una entrada de consola o un socket. En la mayoría de los orígenes de entrada, los datos devueltos son ilimitados en términos de contenido y longitud. Cuando se deselecciona una entrada, se considera que está corrupta.

Algunos ejemplos de probabilidad incluyen:

- Dado un rastreo con un origen HTTP (por ejemplo, `Request.getQueryString`) y un receptor de script entre sitios (por ejemplo, `Response.write`), se ha determinado una probabilidad alta, aumentando así la confianza del resultado.

- Dado un rastreo con un origen de propiedad de sistema (por ejemplo, `getProperty`) y un receptor de script entre sitios (por ejemplo, `Response.write`), se ha determinado una probabilidad baja, disminuyendo así la confianza del resultado.

La probabilidad se utiliza para identificar resultados accionables de prioridad alta que deben seguir o que se deben arreglar inmediatamente. Está unida a orígenes altamente explotables de corrupción y puede proporcionarle un enfoque más preciso para clasificar resultados. La probabilidad se almacena como un atributo que está unido a un origen de corrupción, en la base de datos de vulnerabilidad de AppScan Source. La característica está disponible de forma predeterminada.

Hemos llevado a cabo una búsqueda exhaustiva para determinar el factor de probabilidad para los orígenes. Mediante el uso del Asistente de reglas personalizadas, puede añadir información de probabilidad a nuevos orígenes de corrupción que añade a la base de la regla. Esto mejorará la clasificación de resultados generados desde un escaneo y, a su vez, mejora la eficiencia del flujo de trabajo de asignación de prioridades global.

En el Asistente de reglas personalizadas, hay dos valores (**Alto** y **Bajo**) que puede establecer para la propiedad **Probabilidad**. Un valor de **Alto** significa que el origen es muy susceptible de corromperse. En otras palabras, la barrera para corromper la entrada al sistema es muy baja, lo que facilita que los atacantes envíen datos maliciosos de forma manual o automatizada. Un valor de **Bajo** significa que la barrera para introducir datos maliciosos mediante este origen es muy alta. Ello podría significar que, para que se introduzca corrupción en el origen, un atacante tendría que saber cómo funciona el sistema desde dentro y tener permisos para operar en la red de la víctima.

**Nota:** Como resultado de estos atributos de reglas, si ha generado asesoramientos en versiones anteriores de AppScan Source, puede encontrar que las clasificaciones de búsqueda para el mismo origen se han modificado cuando se ha escaneado en la Versión 9.0.3. Para obtener más información, y para obtener más información sobre cómo inhabilitar estos atributos de reglas, consulte las consideraciones de migración con respecto a estos cambios.

## La resolución automática de receptor perdido permite mejores resultados de escaneo

AppScan Source ahora intenta resolver receptores perdidos en rastreos infiriendo de forma automática en la marcación para los métodos de receptor perdido, como por ejemplo métodos de obtención, de establecimiento, y métodos que devuelven valores booleanos. Esto permite un análisis más minucioso del código y una resolución de receptores perdidos mejorada.

**Nota:** Como resultado de esta característica, si ha generado asesoramientos en versiones anteriores de AppScan Source, puede encontrar un cambio en los resultados de búsqueda para los receptores perdidos que no se han resuelto. Para obtener más información, y para saber cómo inhabilitar la generación de marcación automática, consulte las consideraciones de migración con respecto a estos cambios.

## Nuevo soporte de escaneo mejorado

- PHP Versión 5.4 ahora se puede escanear en Windows y Linux en IBM Security AppScan Source for Analysis, IBM Security AppScan Source for Automation y la interfaz de línea de mandatos (CLI) de IBM Security AppScan Source.

- Ahora AppScan Source incluye soporte integrado para la infraestructura Spring MVC 4.
- **Optimizaciones de escaneo de Java:**
  - Al escanear JavaServer Pages, ahora tiene la opción de escanear archivos de clase precompilados en lugar de compilarlos durante un escaneo. Para escanear archivos de clase precompilados en el Plugin AppScan Source for Development Eclipse , configure el proyecto para el escaneo de seguridad (seleccione **Análisis de seguridad > Configurar escaneo > Configurar proyectos para seguridad**) y seleccione el recuadro **Clases precompiladas**. Para escanear archivos de clase precompilados en IBM Security AppScan Source for Analysis, seleccione el recuadro **Clases precompiladas** en una de estas ubicaciones:
    - El separador Dependencias del proyecto en las propiedades del proyecto.
    - La página Dependencias del proyecto Java al crear un nuevo proyecto o aplicación.
  - Al escanear Java, AppScan Source ahora escanearán archivos Java y código de bytes de Java con dependencias o errores de compilación perdidos. Si hay errores de compilación o faltan dependencias, se grabará la información sobre los mismos en un archivo de registro. Con esta información, podrá añadir las dependencias a las propiedades de proyecto, volver a escanear y conseguir una cobertura completa de los resultados de escaneo.
- A partir de AppScan Source Versión 9.0.3, las ubicaciones de las cabeceras y las opciones de configuración se determinan con más precisión cuando se importan y escanean proyectos Xcode. Este cambio introduce el uso de xcodebuild -dry-run para obtener la configuración de construcción de cada archivo, de modo que es posible que se produzca una pausa al inicio del escaneo mientras AppScan Source determina las configuraciones de construcción antes de continuar.

## **Prestaciones y características que ya no están soportadas en AppScan Source Versión 9.0.3**

A partir de AppScan Source Versión 9.0.3:

- OS X Versión 10.8 ya no es un sistema operativo soportado.
- La versión 4.6 de Xcode ya no está soportada. Ya no está soportado escanear proyectos Objective-C con esta versión de Xcode.
- Deja de darse soporte a espacios de trabajo y archivos de proyecto de Eclipse Versión 3.6 y 3.7. AppScan Source for Development (plugin de Eclipse) ya no se puede aplicar a Eclipse Versiones 3.6 y 3.7.
- Deja de darse soporte a espacios de trabajo y archivos de proyecto de Rational Application Developer for WebSphere Software (RAD) Versión 8.0.x. IBM Security AppScan Source for Development Plug-in for IBM Rational Application Developer for WebSphere Software (RAD) ya no se puede aplicar a RAD Versión 8.0.x.
- IBM Rational Team Concert Versiones 3.0 y 3.0.1 ya no son sistemas de seguimiento de defectos soportados.
- WebSphere Application Server Versión 6.1 ya no es un servidor de aplicaciones soportado.
- El soporte para el escaneo de PHP Versiones 4.x hasta la 5.2 está en desuso.

---

## Migración a la versión actual de AppScan Source

Este tema contiene información acerca de la migración de los cambios realizados en esta versión de AppScan Source. Si está actualizando desde una versión anterior de AppScan Source, asegúrese de tener en cuenta los cambios de la versión de AppScan Source que está actualizando y de todas las versiones que lleven hasta esta versión actual.

- “Migración desde la Versión 9.0.2”
- “Migración desde la versión 9.0” en la página 16
- “Migración desde la versión 8.7” en la página 17

### Migración desde la Versión 9.0.2

- “Los atributos de regla nueva pueden dar lugar a búsquedas de cambios de clasificación en escaneos existentes”
- “Generación de receptor perdido automática” en la página 16

### Los atributos de regla nueva pueden dar lugar a búsquedas de cambios de clasificación en escaneos existentes

Tras la Versión 9.0.2, se introdujeron los atributos de regla `Attribute.Likelihood.High` y `Attribute.Likelihood.Low`. Cuando se utilicen estos atributos, AppScan Source puede determinar de forma más precisa si las búsquedas son definitivas y/o sospechosas. Como resultado, si escanea el código de origen en AppScan Source Versión 9.0.2 o anterior, es posible que descubra que algunas clasificaciones de resultados cambian con el mismo código de origen que se escanea en las versiones del producto tras la 9.0.2. Esto será más perceptible para búsquedas relacionadas con orígenes web altamente explotados, o para los orígenes de entorno o de propiedades que están menos explotados.

Estos atributos de reglas se utilizan de forma predeterminada. Puede inhabilitarlos, como se muestra a continuación:

1. Abra `<data_dir>\config\ipva.ozsettings` en un editor de textos (donde `<data_dir>` es la ubicación de los datos de programa AppScan Source, como se describe en “Instalación y ubicaciones de archivo de datos de usuario” en la página 335). Ubique el valor `allow_likelihoood` en el archivo. Este valor es similar a:

```
<Setting
  name="allow_likelihoood"
  value="true"
  default_value="true"
  description="Permitir el proceso de los atributos Likelihood
    para ayudar a determinar la confianza de rastreo en función
    de la API de origen"
  display_name="Allow Likelihood"
  type="bool"
/>
```

En este valor, modifique el atributo `value`. Si el atributo se establece en `true`, este valor estará activo. Si se establece en `false`, AppScan Source no utilizará estos atributos de reglas durante los escaneos.

2. Guarde el archivo una vez que haya modificado este valor e inicie o reinicie AppScan Source.

## Generación de receptor perdido automática

Tras la Versión 9.0.2, se ha introducido la resolución de receptor perdido automática para rastreos que acaban en métodos get/set y métodos que devuelven valores booleanos. Se realiza infiriendo de forma automática en la marcación para estas interfaces de programa de aplicación (API). Como resultado, si escanea código de origen en AppScan Source Versión 9.0.2 o anterior, es posible que descubra cambios en los resultados de la búsqueda que contenían receptores perdidos no resueltos cuando el mismo código de origen se escanea en las versiones de producto posteriores a 9.0.2.

La generación de marcación automática está activa de forma predeterminada. Puede inhabilitarla si desea utilizar otros medios de resolución de receptor perdido como por ejemplo reglas personalizadas, como se indica a continuación:

1. Abra <data\_dir>\config\ipva.ozsettings en un editor de textos (donde <data\_dir> es la ubicación de los datos de programa AppScan Source, como se describe en “Instalación y ubicaciones de archivo de datos de usuario” en la página 335). Localice el valor automatic\_lost\_sink\_resolution en el archivo. Este valor es similar a:

```
<name="automatic_lost_sink_resolution"
  value="true"
  default_value="true"
  description="Este valor intenta realizar la resolución automática
    de receptor perdido asumiendo la propagación corrupta
    para métodos get, set y API que devuelven booleano
    sin argumentos".
  display_name="Resolución automática de receptor perdido"
  type="bool"
/>
```

En este valor, modifique el atributo value. Si el atributo se establece en true, este valor estará activo. Si se establece en false, AppScan Source no generará de forma automática la marcación para estos métodos.

2. Guarde el archivo una vez que haya modificado este valor e inicie o reinicie AppScan Source.

## Migración desde la versión 9.0

### **Autenticación de AppScan Enterprise Server: Consideraciones acerca de la migración para sustituir el componente de autenticación de usuarios de IBM Rational Jazz por IBM WebSphere Liberty**

- **Migración desde un Enterprise Server que solo tiene usuarios de Jazz locales:**  
En este caso de uso de actualización, los usuarios de Jazz anteriores aparecerán en la base de datos de AppScan Source como usuarios de AppScan Enterprise Server, sin embargo, no serán válidos. Estos usuarios se pueden eliminar de la base de datos o se pueden convertir en usuarios de AppScan Source siguiendo las instrucciones de <http://www.ibm.com/support/docview.wss?uid=swg21686347> para habilitar esta conversión.
- **Migración desde un Enterprise Server que se ha configurado con LDAP:**  
Durante la actualización de Enterprise Server, tiene la opción de volver a configurar el Enterprise Server con LDAP. Si lo hace, los usuarios existentes continuarán funcionando en AppScan Source.
- **Migración desde un Enterprise Server que se ha configurado con la autenticación de Windows:** Si su Enterprise Server se ha configurado con la



autenticación de Windows, los usuarios existentes funcionarán en AppScan Source, siempre que el nuevo Enterprise Server Liberty se haya configurado para utilizar la autenticación de Windows.

## Migración desde la versión 8.7

- “Cambios en las clasificaciones de los resultados”
- “Cambios en los valores predeterminados que mejorarán la cobertura del escaneo” en la página 18
- “Restauración de filtros predefinidos de AppScan Source de versiones anteriores” en la página 18

### Cambios en las clasificaciones de los resultados

A partir de la versión 8.7, han cambiado los resultados de las clasificaciones. En esta tabla se muestra una lista de las clasificaciones anteriores correlacionadas con las nuevas clasificaciones:

Tabla 1. Cambios en la clasificación de los resultados

| Clasificaciones de resultados anteriores a AppScan Source Versión 8.8 | Clasificaciones a partir de AppScan Source Versión 8.8 |
|-----------------------------------------------------------------------|--------------------------------------------------------|
| Vulnerabilidad                                                        | Resultado de seguridad definitivo                      |
| Excepción tipo I                                                      | Resultado de seguridad sospechoso                      |
| Excepción tipo II                                                     | Resultado de cobertura de escaneo                      |

En la vista de la matriz de vulnerabilidad encontrará un ejemplo de estos cambios.

| Reset  | Vulnerability | Exceptions |         | Totals |
|--------|---------------|------------|---------|--------|
|        |               | Type I     | Type II |        |
| High   | 0             | 51         | 0       | 51     |
| Medium | 0             | 12         | 5       | 17     |
| Low    | 0             | 67         | 3       | 70     |
| Totals | 0             | 130        | 8       | 138    |

A partir de la Versión 8.8, la vista es la siguiente:

|        | Security Findings |         | Scan Coverage Findings | Totals |
|--------|-------------------|---------|------------------------|--------|
|        | Definitive        | Suspect |                        |        |
| High   | 0                 | 51      | 0                      | 51     |
| Medium | 0                 | 16      | 5                      | 21     |
| Low    | 0                 | 81      | 9                      | 90     |
| Totals | 0                 | 148     | 14                     | 162    |

## Cambios en los valores predeterminados que mejorarán la cobertura del escaneo

A partir de AppScan Source Versión 8.8:

- El valor predeterminado de `show_informational_findings` en `scan.ozsettings` ha cambiado de `true` a `false`.
- El valor predeterminado de `waf_globals_tracking` en `ipva.ozsettings` ha cambiado de `false` a `true`. Este valor habilita a AppScan Source a encontrar flujos de datos entre diferentes componentes de una aplicación basada en una infraestructura (por ejemplo, un flujo de datos desde un controlador a una vista).

El cambio a `show_informational_findings` dará lugar a asesoramientos que de forma predeterminada no incluirán resultados con un nivel de gravedad de **Info**.

**Nota:** Si tiene configuraciones de escaneo que se han creado antes de la Versión 8.8 que no establecieron explícitamente valores para estos valores, las configuraciones de escaneo ahora utilizarán sus nuevos valores predeterminados.

## Restauración de filtros predefinidos de AppScan Source de versiones anteriores

En AppScan Source Versión 8.8, se mejoraron los filtros predefinidos para proporcionar mejores resultados de escaneo. Si necesita continuar utilizando los filtros predefinidos de versiones anteriores de AppScan Source (los filtros archivados se encuentran listados en “Filtros predefinidos de AppScan Source (Versión 8.7.x y anteriores)” en la página 159), siga las instrucciones en “Restauración de filtros predefinidos archivados” en la página 161.

---

## Visión general de AppScan Source for Analysis

AppScan Source for Analysis es una herramienta para analizar código y ofrecer información específica sobre las vulnerabilidades del código fuente en sistemas críticos. AppScan Source for Analysis permite gestionar de forma centralizada el riesgo del software entre varias aplicaciones, incluso entre un portfolio completo. Puede escanear código fuente, seleccionar y eliminar vulnerabilidades antes de que supongan un riesgo para la organización.

AppScan Source for Analysis proporciona a los equipos de protección de auditoría y calidad, herramientas para escanear el código fuente, seleccionar resultados y enviar fallos a los sistemas de seguimiento de defectos.

Con la inteligencia incorporada que proporciona la Base de datos de conocimientos de AppScan Source Security, los analistas, auditores, gestores y desarrolladores pueden:

- Escanear el código fuente seleccionado según demanda para localizar vulnerabilidades críticas
- Recibir consejos precisos sobre remediación e invocar el entorno de desarrollo y el editor de código que deseen directamente desde la fase de análisis
- Realizar un rastreo de datos corruptos a través de un gráfico de llamadas preciso e interactivo entre entrada y salida
- Imponer políticas de codificación, verificando las rutinas de validación y codificación de entrada aprobadas a través del rastreo de AppScan Source
- Aprender e implementar prácticas recomendadas de programación segura durante el desarrollo del software

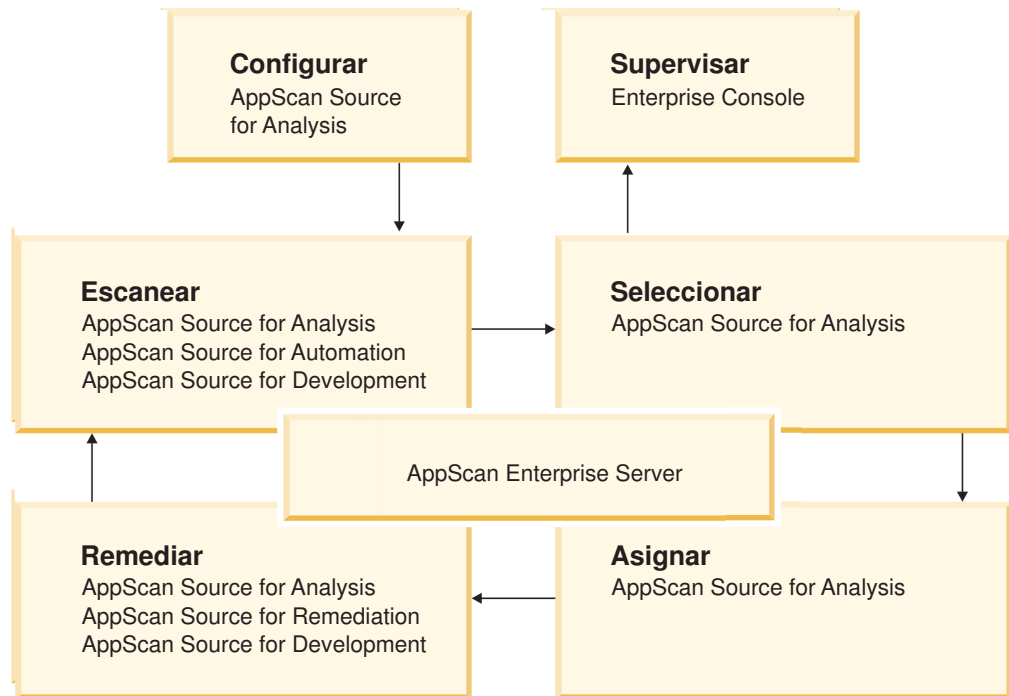
---

## Flujo de trabajo

Tras la instalación, despliegue y gestión de usuarios, el flujo de trabajo de AppScan Source consta de estos pasos básicos.

1. **Establecer requisitos de seguridad:** un gestor o experto en seguridad define vulnerabilidades y cómo juzgar la importancia de las mismas.
2. **Configurar aplicaciones:** Organice aplicaciones y proyectos.
3. **Escanear:** Ejecute el análisis de la aplicación de destino para identificar vulnerabilidades.
4. **Seleccionar y analizar resultados:** el personal de seguridad estudia los resultados para establecer un flujo de trabajo de remediación prioritario y separar las vulnerabilidades reales de las potenciales, permitiendo que los problemas críticos se comiencen a solucionar de inmediato. Identifique los elementos que necesita arreglar primero.
5. **Personalice la base de datos de conocimientos:** Personalizar la Base de datos de conocimientos de AppScan Source Security para adaptarla a las políticas internas.
6. **Publicar resultados de un escaneo:** Añada los resultados de un escaneo a la base de datos de AppScan Source o publíquelos en AppScan Enterprise Console.
7. **Asignar tareas de solución:** Asigne defectos al equipo de desarrollo para resolver vulnerabilidades.
8. **Resolver problemas:** Elimine vulnerabilidades al reescribir el código, al eliminar errores o al añadir funciones de seguridad.

9. **Verificar arreglos:** se vuelve a escanear el código para asegurarse de que las vulnerabilidades se han eliminado.



## Conceptos importantes

Antes de empezar a utilizar o administrar AppScan Source, debe familiarizarse con los conceptos fundamentales de AppScan Source. En esta sección se definen la terminología y los conceptos básicos de AppScan Source. En los siguientes capítulos se repiten estas definiciones para ayudarle a comprender su contexto en AppScan Source for Analysis.

AppScan Source for Analysis *escanea* código fuente en busca de vulnerabilidades y genera *resultados*. Los resultados son las vulnerabilidades identificadas durante un escaneo y el resultado de un escaneo es un *asesoramiento*. Un *paquete* es una colección con nombre de resultados individuales y se almacena con una aplicación.

Las aplicaciones, sus atributos y los proyectos se crean y se organizan en AppScan Source for Analysis:

- **Aplicaciones:** una aplicación contiene uno o varios proyectos y sus atributos relacionados.
- **Proyectos:** un proyecto consta de un conjunto de archivos (incluido el código fuente) y su información relacionada (como por ejemplo datos de configuración). Un proyecto siempre forma parte de una aplicación.
- **Atributos:** un atributo es una característica de una aplicación que ayuda a organizar los resultados de un escaneo en grupos significativos, como por ejemplo por departamento o por gestor de proyecto. El usuario define atributos en AppScan Source for Analysis.

La principal actividad de AppScan Source for Analysis consiste en escanear el código fuente y en analizar las vulnerabilidades. Los asesoramientos proporcionan un análisis del código fuente en busca de vulnerabilidades e incluyen:

- **Gravedad:** alta, media o baja, que indica el nivel de riesgo
- **Tipo de vulnerabilidad:** categoría de la vulnerabilidad, como por ejemplo Inyección de SQL o Desbordamiento de almacenamiento intermedio
- **Archivo:** archivo de código en que se da el resultado
- **API/Origen:** la llamada vulnerable, que muestra la API y los argumentos pasados a la misma
- **Método:** función o método desde el que se realiza la llamada vulnerable
- **Ubicación:** número de línea y columna en el archivo de código que contiene la API vulnerable
- **Clasificación:** resultado de seguridad o resultado de cobertura de escaneo. Para obtener más información, consulte “Clasificaciones”.

## Clasificaciones

AppScan Source clasifica los resultados para indicar si se trata de resultados de cobertura de escaneo o de seguridad. Los resultados de seguridad representan vulnerabilidades de seguridad reales o probables, mientras que los resultados de cobertura de escaneo representan áreas donde la configuración se podría mejorar para una mejor cobertura del escaneo.

Cada resultado estará dentro de una de estas *clasificaciones*:

- Resultado de seguridad **definitivo**: un resultado que contiene un diseño definitivo, implementación o violación de política que presenta una oportunidad para que un atacante haga que la aplicación funcione de forma no deseada. Este ataque podría dar lugar a un acceso no autorizado, robo o daño en los datos, sistemas o recursos. Cada resultado de seguridad definitivo se articula totalmente, y el patrón subyacente específico de la condición vulnerable se sabe y describe.
- Resultado de seguridad **sospechoso**: un resultado que indica una condición vulnerable potencialmente y sospechosa que requiere de investigación o información adicional. Un elemento o estructura de código que puede crear una vulnerabilidad cuando se utiliza incorrectamente.  
Un resultado sospechoso difiere de un resultado definitivo en que hay alguna condición desconocida que impide una determinación concluyente de vulnerabilidad. Ejemplos de esta incertidumbre pueden ser el uso de elementos dinámicos o funciones de biblioteca para las que el código fuente no está disponible. Como resultado, hay un nivel adicional de investigación necesaria para confirmar o rechazar un resultado sospechoso como definitivo.
- Resultado de **cobertura de escaneo**: resultados que representan áreas en las que la configuración se podría mejorar para proporcionar una mejor cobertura del escaneo (por ejemplo, resultados de salidas perdidas (sink)).

**Nota:** En algunos casos, se puede utilizar una clasificación de **Ninguno** para denotar una clasificación que no corresponde a un resultado de seguridad ni a un resultado de cobertura de escaneo.

---

## Inicio de sesión en AppScan Enterprise Server desde productos AppScan Source

La mayoría de los productos y componentes de AppScan Source requieren una conexión a un AppScan Enterprise Server. El servidor ofrece funciones de gestión de usuario centralizadas y un mecanismo para compartir asesoramientos a través de la base de datos de AppScan Source.

Al iniciar AppScan Source for Analysis, se le solicitará que se autentique en una instancia de AppScan Enterprise Server. Si AppScan Source for Development se ejecuta en modo de servidor, se le solicitará que se autentique en una instancia de AppScan Enterprise Server cuando inicie una sesión la primera vez que inicie una acción en la que sea necesario acceder al servidor como, por ejemplo, al lanzar un escaneo o visualizar configuraciones de escaneo.

- “Iniciando una sesión desde AppScan Source for Analysis y AppScan Source for Development con un ID de usuario y contraseña de AppScan Enterprise Server”
- “Utilización de la autenticación con CAC (Common Access Card) para iniciar una sesión desde AppScan Source for Analysis y AppScan Source for Development” en la página 23
- “Inicio de sesión desde AppScan Source for Automation y la interfaz de línea de mandatos (CLI) de AppScan Source” en la página 24
- “Certificados SSL de AppScan Enterprise Server” en la página 24
- “Resolución de errores de certificado de AppScan Enterprise Server” en la página 24

## **Iniciando una sesión desde AppScan Source for Analysis y AppScan Source for Development con un ID de usuario y contraseña de AppScan Enterprise Server**

En AppScan Source for Analysis, cuando inicie la sesión se le solicitará:

- **ID de usuario:** Especifique su ID de usuario (en función de cómo se haya configurado la cuenta, se trata de un ID de usuario que existe tanto en AppScan Enterprise Server como en la base de datos de AppScan Source - o puede ser un ID de usuario que solo exista en la base de datos de AppScan Source).
  - Si se ha configurado AppScan Enterprise Server para utilizar la autenticación de Windows, escriba el dominio y el nombre de usuario que utiliza para conectarse con Enterprise Console (separe el dominio y el nombre de usuario con una barra invertida, \, por ejemplo, mi\_dominio\mi\_nombreusuario).
  - Si se ha configurado AppScan Enterprise Server con LDAP, escriba el nombre de usuario que ha utilizado para conectarse con Enterprise Console.
- **Contraseña:** Especifique la contraseña para el ID de usuario.
- **AppScan Enterprise Server:** Especifique el URL para la instancia de AppScan Enterprise Server. El formato de este URL es `http(s)://<nombrehost>:<puerto>/ase`, donde `<nombrehost>` es el nombre de la máquina en que se ha instalado AppScan Enterprise Server y `<puerto>` es el puerto en que el servidor está en ejecución. Un ejemplo de este URL podría ser `https://myhost.mydomain.ibm.com:9443/ase`.

En AppScan Source for Development, cuando inicie la sesión se le solicitará:

- **URL de servidor:** Especifique el URL para la instancia de AppScan Enterprise Server. El formato de este URL es `http(s)://<nombrehost>:<puerto>/ase`, donde `<nombrehost>` es el nombre de la máquina en que se ha instalado AppScan Enterprise Server y `<puerto>` es el puerto en que el servidor está en ejecución. Un ejemplo de este URL podría ser `https://myhost.mydomain.ibm.com:9443/ase`.
- **ID de usuario:** Especifique su ID de usuario (en función de cómo se haya configurado la cuenta, se trata de un ID de usuario que existe tanto en AppScan Enterprise Server como en la base de datos de AppScan Source - o puede ser un ID de usuario que solo exista en la base de datos de AppScan Source).
  - Si se ha configurado AppScan Enterprise Server para utilizar la autenticación de Windows, escriba el dominio y el nombre de usuario que utiliza para

- conectarse con Enterprise Console (separe el dominio y el nombre de usuario con una barra invertida, \, por ejemplo, mi\_dominio\mi\_nombreusuario).
- Si se ha configurado AppScan Enterprise Server con LDAP, escriba el nombre de usuario que ha utilizado para conectarse con Enterprise Console.
- **Contraseña:** Especifique la contraseña para el ID de usuario.

## Utilización de la autenticación con CAC (Common Access Card) para iniciar una sesión desde AppScan Source for Analysis y AppScan Source for Development

En Windows, se puede conectar a una instancia de AppScan Enterprise Server utilizando la autenticación con CAC (<http://www.cac.mil>). Antes de hacer esto, debe configurar AppScan Enterprise Server y AppScan Source para la autenticación con CAC (Common Access Card). Si Enterprise Server está configurado para la autenticación CAC, no puede utilizar un ID de usuario ni su contraseña de Enterprise Server para iniciar una sesión.

En AppScan Source for Analysis, cuando inicie la sesión se le solicitará:

- **Usuario:** Seleccione su nombre común de CAC de la lista.
- **AppScan Enterprise Server:** Especifique el URL para la instancia de AppScan Enterprise Server. El formato de este URL es `http(s)://<nombrehost>:<puerto>/ase`, donde `<nombrehost>` es el nombre de la máquina en que se ha instalado AppScan Enterprise Server y `<puerto>` es el puerto en que el servidor está en ejecución. Un ejemplo de este URL podría ser `https://myhost.mydomain.ibm.com:9443/ase`.

En AppScan Source for Development, cuando inicie la sesión se le solicitará:

- **URL de servidor:** Especifique el URL para la instancia de AppScan Enterprise Server. El formato de este URL es `http(s)://<nombrehost>:<puerto>/ase`, donde `<nombrehost>` es el nombre de la máquina en que se ha instalado AppScan Enterprise Server y `<puerto>` es el puerto en que el servidor está en ejecución. Un ejemplo de este URL podría ser `https://myhost.mydomain.ibm.com:9443/ase`.
- **Usuario:** Seleccione su nombre común de CAC de la lista.

Después de pulsar **Aceptar**, se le solicitará mediante un recuadro de diálogo de seguridad de Windows su número secreto de la tarjeta CAC.

### Consejo:

- Si el inicio de sesión falla, asegúrese de que AppScan Enterprise Server está correctamente configurado y de que su certificado es válido. Compruebe si puede acceder a AppScan Enterprise Server a través de un navegador. Si es así, debería poder seleccionar el certificado e iniciar una sesión.
- Si el campo del recuadro de diálogo de inicio de sesión de **Usuario** no muestra una lista con los certificados disponibles, asegúrese de que ha modificado el archivo `java.security` en su JRE, tal como se describe en “Habilitación de la autenticación con CAC (Common Access Card)” en la página 24.
- Si no aparece un recuadro de diálogo de seguridad de Windows solicitándole el pin de su tarjeta CAC, asegúrese de que el servicio Microsoft Smart Card Resource Manager está en ejecución. Tenga en cuenta es posible que este servicio no se ejecute en algunos tipos de conexión de escritorio remoto.

## Inicio de sesión desde AppScan Source for Automation y la interfaz de línea de mandatos (CLI) de AppScan Source

También se necesitan acciones de inicio de sesión cuando se ejecuta AppScan Source for Automation o la interfaz de línea de mandatos (CLI) de AppScan Source. Consulte el manual *IBM Security AppScan Source Utilities Guía del usuario* para obtener más información.

## Certificados SSL de AppScan Enterprise Server

Para obtener información sobre certificados SSL de AppScan Enterprise Server, consulte “Certificados SSL de AppScan Enterprise Server” en la página 26.

## Resolución de errores de certificado de AppScan Enterprise Server

Si ha iniciado una sesión en una instancia de Enterprise Server con una autoridad de certificados desconocida, recibirá una excepción relacionada con el certificado o un error después de iniciar la sesión. AppScan Source incluye un pequeño programa de utilidad que puede ayudarle a corregir esta situación. La herramienta es `<dir_instalación>\bin\certificatetool.bat` (donde `<dir_instalación>` es la ubicación de la instalación de AppScan Source) - o `<dir_instalación>/bin/certificatetool.sh` en Linux y macOS.

## Habilitación de la autenticación con CAC (Common Access Card)

Este tema sirve para configurar AppScan Source para que permita conectarse a una instancia de AppScan Enterprise Server que esté habilitada para la autenticación con CAC (Common Access Card).

### Antes de empezar

Únicamente se da soporte a la autenticación con CAC en Windows con conexiones a AppScan Enterprise Server Versión 9.0.3.1 iFix-001 y superior.

### Procedimiento

1. Asegúrese de que todavía no se ha configurado a AppScan Enterprise Server para la autenticación con CAC.
2. Inicie una sesión en AppScan Source for Analysis o en la interfaz de línea de mandatos (CLI) de AppScan Source como un administrador de AppScan Source.
3. Siga las instrucciones en la *IBM Security AppScan Source Guía de instalación y administración* para configurar a todos los usuarios de AppScan Enterprise Server para que tengan todos los permisos. Esto establecerá los permisos predeterminados iniciales para los usuarios de AppScan Enterprise Server con acceso completo administrativo, sin embargo, una vez se haya completado la configuración de CAC, podrá cambiar los permisos predeterminados para que se adecúen a las necesidades de su organización.
4. Salga o concluya todas las aplicaciones de cliente de AppScan Source.
5. Configuración de AppScan Enterprise Server para permitir la autenticación con CAC
6. Siga las instrucciones en la *IBM Security AppScan Source Guía de instalación y administración* para registrar la base de datos de AppScan Source con una



instancia de AppScan Enterprise Server que esté habilitada para la autenticación con CAC (Common Access Card).

7. Abra <dir\_datos>\config\ounce.ozsettings (donde <data\_dir> es la ubicación de los datos de programa AppScan Source, como se describe en “Instalación y ubicaciones de archivo de datos de usuario” en la página 335)). En este archivo, localice este valor:

```
<Setting
  name="client_cert_auth"
  value="false"
  default_value="false"
  description="Uses client certificate authentication"
  display_name="Uses client certificate authentication"
  type="boolean"
  read_only="true"
  hidden="true"
/>
```

8. En el valor, cambie value="false" por value="true" y, a continuación, guarde el archivo.
9. Si se conectará en AppScan Enterprise Server desde AppScan Source for Analysis o el Plugin AppScan Source for Development Eclipse :
  - a. En su directorio de instalación de Java, encuentre el archivo jre/lib/security/java.security. En AppScan Source for Analysis, la carpeta jre se encuentra en su directorio de instalación de AppScan Source. Cree una copia de seguridad de este archivo.
  - b. Edite java.security.
  - c. En la lista de proveedores y su orden de preferencias, añada com.ibm.security.capi.IBMCAC como el primer proveedor de seguridad. Por ejemplo, si está editando java.security para la utilización de AppScan Source for Analysis, cambie esto:

```
security.provider.1=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.2=com.ibm.jsse2.IBMJSSEProvider2
security.provider.3=com.ibm.crypto.provider.IBMJCE
security.provider.4=com.ibm.security.cert.IBMCertPath
security.provider.5=sun.security.provider.Sun
```

por esto:

```
security.provider.1=com.ibm.security.capi.IBMCAC
security.provider.2=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.3=com.ibm.jsse2.IBMJSSEProvider2
security.provider.4=com.ibm.crypto.provider.IBMJCE
security.provider.5=com.ibm.security.cert.IBMCertPath
security.provider.6=sun.security.provider.Sun
```
  - d. Guarde y cierre el archivo java.security.
10. Inicie una sesión como un administrador de AppScan Source para AppScan Source for Analysis o la interfaz de línea de mandatos (CLI) de AppScan Source utilizando la autenticación con CAC.
11. Cambie los permisos predeterminados de los usuarios de AppScan Enterprise Server para que se adecúen a las necesidades de su organización.

## Qué hacer a continuación

Su certificado no puede ser de tipo SHA-1 si desea imponer la modalidad FIPS (Federal Information Processing Standard). Es posible imponer la modalidad FIPS utilizando un certificado SHA-2 y ejecutando la herramienta appscanserverdbmgr\_cac\_fips.bat que se describe en la *IBM Security AppScan Source Guía de instalación y administración*. En la guía, encuentre la ayuda para

registrar la base de datos de AppScan Source con una instancia de AppScan Enterprise Server habilitada con autenticación con CAC (Common Access Card).

Para determinar qué certificados posee:

1. Abra el Administrador de certificados de Windows: En el menú Inicio de Windows, escriba `certmgr.msc` en el recuadro de búsqueda y, a continuación, pulse Intro. Si se le solicita una contraseña de administrador o confirmación, especifique la contraseña o proporcione la confirmación.
2. Abra el certificado realizando una doble pulsación o mediante la acción **Abrir** de la interfaz de usuario.
3. Seleccione el separador Detalles en el certificado.
4. Busque el campo **Algoritmo hash de firma**. El valor de este campo indica el tipo de certificado.

## Modificación de las contraseñas de usuario de AppScan Source

Para poder cambiar una contraseña de usuario de AppScan Source, debe tener permiso para **Gestionar usuarios** y el cambio se debe realizar en AppScan Source for Analysis. Si no tiene este permiso, solicite a su administrador que le cambie la contraseña, siguiendo las instrucciones de este tema. Si AppScan Enterprise Server está configurado para utilizar la autenticación LDAP o la autenticación Windows, este tema no se aplica.

### Procedimiento

1. En AppScan Source for Analysis, seleccione **Admin > Gestionar usuarios** en el menú principal del entorno de trabajo.
2. El recuadro de diálogo Gestionar usuarios incluye una lista de los usuarios de AppScan Source existentes. Para cambiar la contraseña de uno de estos usuarios, edite la información del usuario realizando una de estas tareas:
  - Pulse dos veces el usuario.
  - Pulse con el botón derecho el usuario y seleccione **Editar usuario**.
  - Seleccione el usuario y pulse el botón **Editar usuario**.

**Nota:** No puede cambiar la contraseña de un usuario de AppScan Enterprise Server desde AppScan Source.

3. En el recuadro de diálogo Editar usuario, escriba una contraseña nueva y, a continuación, vuelva a escribir la contraseña en el campo **Confirmar contraseña**.
4. Pulse en **Aceptar** para guardar la contraseña.

## Certificados SSL de AppScan Enterprise Server

Cuando se instala AppScan Enterprise Server, se debe configurar de modo que utilice un certificado SSL válido. Si no se hace, recibirá un mensaje de conexión no fiable cuando inicie la sesión en el servidor desde AppScan Source for Analysis o la interfaz de línea de mandatos (CLI) de AppScan Source - en AppScan Source for Development en Windows y Linux.

### Ubicación del almacenamiento de certificados SSL

Los certificados que se han aceptado de forma permanente se guardan en `<data_dir>\config\cacertspersonal` y `<data_dir>\config\cacertspersonal.pem` (donde `<data_dir>` es la ubicación de los datos de programa AppScan Source,

como se describe en “Instalación y ubicaciones de archivo de datos de usuario” en la página 335). Elimine estos dos archivos si ya no desea guardar de forma permanente los certificados.

## **Validación de certificados de AppScan Source for Automation y SSL**

De forma predeterminada, los certificados se aceptan de forma permanente cuando se utiliza AppScan Source for Automation. Este comportamiento viene determinado por el valor `ounceautod_accept_ssl` del archivo de configuración de servidor de automatización (`<data_dir>\config\ounceautod.ozsettings` (donde `<data_dir>` es la ubicación de los datos de programa AppScan Source, como se describe en “Instalación y ubicaciones de archivo de datos de usuario” en la página 335)). Si este valor se edita y se establece `value="true"` en `value="false"`, se intentará la validación SSL y el inicio de sesión o la publicación en AppScan Enterprise Console fallarán con un error si se encuentra un certificado no válido.

## **Validación de certificados de interfaz de línea de mandatos (CLI) de AppScan Source y SSL**

De forma predeterminada, cuando se utiliza el mandato `login` de la interfaz de línea de mandatos, se intentará la validación SSL y el intento de inicio de sesión o el intento de publicación fallará si se encuentra un certificado no válido (si todavía no ha aceptado de forma permanente el certificado al iniciar una sesión a través de otro producto de cliente de AppScan Source). Se puede modificar este comportamiento utilizando el parámetro `-acceptssl` de la opción al emitir el mandato `login`. Al utilizar este parámetro, se aceptan automáticamente los certificados SSL.

---

## **AppScan Source y accesibilidad**

La accesibilidad afecta a los usuarios con discapacidades físicas, como movilidad restringida o visión limitada. Los problemas de accesibilidad pueden impedir el uso correcto de productos de software. Este tema muestra los problemas conocidos de accesibilidad de AppScan Source y sus soluciones temporales.

## **Utilización de JAWS Screen Reading Software con el instalador de AppScan Source**

Para utilizar Freedom Scientific JAWS (<http://www.freedomscientific.com/products/fs/jaws-product-page.asp>) al ejecutar el instalador de AppScan Source, debe instalar Java Access Bridge en la JVM de AppScan Source. Esto permite que JAWS reproduzca adecuadamente mediante el habla las etiquetas y los controles en los paneles del instalador.

- Encontrará información sobre Java Access Bridge (incluido el enlace de descarga e instrucciones de instalación) en <http://www.oracle.com/technetwork/java/javase/tech/index-jsp-136191.html>.
- Encontrará información sobre el requisito de InstallAnywhere para instalar Java Access Bridge en <http://kb.flexerasoftware.com/selfservice/documentLink.do?externalID=Q200311>.

## Utilización de JAWS Screen Reading Software en paneles de la interfaz de usuario con texto descriptivo

Muchas partes de la interfaz de usuario de AppScan Source contienen texto descriptivo. En la mayoría de los casos, debe utilizar la pulsación de teclas Insertar+B de JAWS para poder leer el texto descriptivo.

---

### Avisos

Esta información se ha desarrollado para productos y servicios ofrecidos en los Estados Unidos. Es posible que en otros países IBM no ofrezca los productos, los servicios o las características que se describen en este documento. Consulte con el representante local de IBM para obtener información acerca de los productos y servicios que actualmente están disponibles en su localidad. Las referencias hechas a productos, programas o servicios IBM no pretenden afirmar ni dar a entender que únicamente puedan utilizarse dichos productos, programas o servicios IBM. Puede utilizarse en su lugar cualquier otro producto, programa o servicio funcionalmente equivalente que no vulnere ninguno de los derechos de propiedad intelectual de IBM. No obstante, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patente pendientes relacionadas con los temas que se describen en este documento. La posesión de este documento no otorga ninguna licencia sobre dichas patentes. Puede enviar las consultas sobre licencias, por escrito, a la siguiente dirección:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785, EE. UU.

Para solicitudes de información sobre licencias referentes a información de juegos de caracteres de doble byte (DBCS), póngase en contacto con el Departamento de propiedad intelectual de IBM de su país, o envíe solicitudes de información, por escrito, a esta dirección:

Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan, Ltd.  
19-21, Nihonbashi-Hakozakicho, Chuo-ku  
Tokio 103-8510, Japón

**El párrafo siguiente no se aplica al Reino Unido ni a ningún otro país donde estas disposiciones sean incompatibles con la legislación vigente:**

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍA DE NINGÚN TIPO, YA SEA EXPLÍCITA O IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN, COMERCIALIZACIÓN O IDONEIDAD PARA UNA FINALIDAD DETERMINADA.

Algunos países no permiten la renuncia a garantías expresas o implícitas en ciertas transacciones, por lo que el párrafo anterior puede no aplicarse en su caso.

Esta información puede contener imprecisiones técnicas o errores tipográficos. Periódicamente, se efectúan cambios en la información incluida en este documento; estos cambios se incorporarán en nuevas ediciones de la publicación. IBM puede efectuar mejoras o cambios en los productos o programas descritos en esta publicación en cualquier momento y sin previo aviso.

Las referencias en esta información a sitios web que no son de IBM se proporcionan solo por conveniencia y bajo ningún concepto se considerarán un anexo a esos sitios web. Los materiales de dichos sitios web no forman parte de este producto de IBM y la utilización de los mismos será por cuenta y riesgo del usuario.

IBM puede utilizar o distribuir la información que usted le suministre del modo que IBM considere conveniente sin incurrir por ello en ninguna obligación para con usted.

Los licenciarios de este programa que deseen obtener información acerca del mismo con el fin de: (i) intercambiar la información entre los programas creados independientemente y otros programas (incluido éste) y (ii) utilizar mutuamente la información que se ha intercambiado, deben ponerse en contacto con:

IBM Corporation  
2Z4A/101  
11400 Burnet Road Austin, TX 78758 EE.UU.

Dicha información puede estar disponible, sujeta a los términos y condiciones adecuados, incluido en algunos casos el pago de una tarifa.

IBM proporciona el programa bajo licencia que se describe en este documento y todo el material bajo licencia disponible para el mismo bajo los términos del Acuerdo del cliente IBM, del Acuerdo Internacional de programas bajo licencia de IBM o de cualquier acuerdo equivalente.

Los datos de rendimiento incluidos aquí se determinaron en un entorno controlado. Por lo tanto, los resultados que se obtengan en otros entornos operativos pueden variar significativamente. Pueden haberse realizado algunas mediciones en sistemas a nivel de desarrollo y no existe ninguna garantía de que estas mediciones vayan a ser equivalentes en sistemas disponibles generalmente. Además, puede que algunas medidas se hayan estimado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables a su entorno específico.

La información concerniente a productos no IBM se ha obtenido de los suministradores de dichos productos, de sus anuncios publicados o de otras fuentes de información pública disponibles. IBM no ha comprobado dichos productos y no puede afirmar la exactitud en cuanto a rendimiento, compatibilidad u otras características relativas a productos no IBM. Las consultas acerca de las posibilidades de los productos no IBM deben dirigirse a los suministradores de los mismos.

Todas las declaraciones relativas a las intenciones futuras de IBM están sujetas a cambios o cancelaciones sin previo aviso y únicamente representan planes y objetivos.

Todos los precios de IBM que se muestran son precios de distribución sugeridos por IBM, actuales y sujetos a cambios sin previo aviso. Los precios de cada comercio específico pueden variar.

Esta información sólo es para fines de planificación. La información está sujeta a cambios antes de que los productos aquí descritos estén disponibles.

Esta información contiene ejemplos de datos e informes utilizados en operaciones comerciales diarias. Para ilustrarlas de la manera más completa posible, los ejemplos incluyen nombres de individuos, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier parecido con los nombres y direcciones utilizados por una empresa real es mera coincidencia.

#### LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de ejemplo en lenguaje fuente, que se utilizan para complementar las explicaciones relacionadas con las técnicas de programación en diversas plataformas operativas. Puede copiar, modificar y distribuir los programas de ejemplo de cualquier forma, sin tener que pagar a IBM, con intención de desarrollar, utilizar, comercializar o distribuir programas de aplicación que estén en conformidad con la interfaz de programación de aplicaciones (API) de la plataforma operativa para la que están escritos los programas de ejemplo. Los ejemplos no se han probado minuciosamente bajo todas las condiciones. Por lo tanto, IBM no puede garantizar ni dar por sentada la fiabilidad, la facilidad de mantenimiento ni el funcionamiento de los programas. Puede copiar, modificar y distribuir estos programas de ejemplo de cualquier forma sin pagar a IBM para los fines de los programas de aplicaciones de desarrollo, uso, marketing o distribución conformes a las interfaces de programación de la aplicación de IBM.

Cada copia o cada parte de los programas de ejemplo o de los trabajos que se deriven de ellos debe incluir un aviso de copyright como se indica a continuación:

© (nombre de la empresa) (año). Algunas partes de este código se derivan de programas de ejemplo de IBM Corp. © Copyright IBM Corp. \_escriba el año o los años\_. Reservados todos los derechos.

Si está consultando esta información en copia software, es posible que no se vean las fotografías y las ilustraciones de color.

### **Marcas registradas**

IBM, el logotipo de IBM y [ibm.com](http://ibm.com) son marcas registradas o marcas comerciales registradas de International Business Machines Corp., patentadas en numerosas jurisdicciones de todo el mundo. Otros nombres de productos y servicios pueden ser marcas registradas de IBM o de otras compañías. Existe una lista actual de marcas registradas de IBM en la web en el apartado "Copyright and trademark information" en [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Adobe, Acrobat, PostScript y todas las marcas basadas en Adobe son marcas registradas de Adobe Systems Incorporated en Estados Unidos y otros países.

IT Infrastructure Library es una marca registrada de Central Computer and Telecommunications Agency, que forma parte de Office of Government Commerce.

Intel, el logotipo de Intel, Intel Inside, el logotipo de Intel Inside, Intel Centrino, el logotipo de Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium y Pentium son marcas registradas de Intel Corporation o de sus subsidiarias en los Estados Unidos y/o en otros países.

Linux es una marca registrada de Linus Torvalds en Estados Unidos o en otros países.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en Estados Unidos y/o en otros países.

ITIL es una marca registrada y una marca registrada comunitaria de OGC (Office of Government Commerce), y está registrada en la Oficina de Patentes y Marcas de Estados Unidos.

UNIX es una marca registrada de The Open Group en Estados Unidos y en otros países.

Java, todas las marcas registradas y logotipos basados en Java son marcas registradas de Oracle y/o sus afiliados.

Cell Broadband Engine es una marca registrada de Sony Computer en Estados Unidos y/o en otros países y se utiliza bajo licencia.

Linear Tape-Open, LTO, el logotipo de LTO, Ultrium y el logotipo de Ultrium son marcas registradas de HP, IBM Corp. y Quantum en EE.UU. y en otros países.

---

## Copyright

(C) Copyright IBM Corp. y sus licenciantes 2003, 2017. All Rights Reserved.

IBM, el logotipo de IBM, ibm.com Rational, AppScan, Rational Team Concert, WebSphere y ClearQuest son marcas registradas o marcas comerciales de International Business Machines Corp. registradas en muchas jurisdicciones de todo el mundo. Otros nombres de servicio y producto podrían ser marcas registradas de IBM u otras compañías. Existe una lista actual de marcas registradas de IBM en la web en el apartado Copyright and trademark information en <http://www.ibm.com/legal/copytrade.shtml>. Linux es una marca registrada de Linus Torvalds en los Estados Unidos y/o en otros países. Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en los Estados Unidos, en otros países o en ambos. Unix es una marca registrada de The Open Group en los Estados Unidos y/o en otros países. Java, todas las marcas registradas y logotipos basados en Java son marcas registradas de Oracle y/o sus afiliados.

Este programa incluye: Jacorb 2.3.0, Copyright 1997-2006 The JacORB project; y XOM1.0d22, Copyright 2003 Elliotte Rusty Harold; cada uno está disponible bajo la licencia Gnu Library General Public License (LGPL) y una copia de la misma está disponible en el archivo de avisos que acompaña a este programa.





---

## Capítulo 2. Configuración de aplicaciones y proyectos

Antes de realizar un escaneo, debe configurar aplicaciones y proyectos. En esta sección se explica el Asistente para aplicaciones nuevas, el Asistente de proyecto nuevo y Application Discovery Assistant. Obtendrá información acerca de cómo configurar los atributos para AppScan Source for Analysis. Además, esta sección le muestra cómo añadir aplicaciones y proyectos existentes al escaneo y cómo añadir archivos a proyectos.

La configuración de AppScan Source for Analysis incluye la creación de una aplicación, la configuración del código fuente y la configuración de atributos. Después de configurar y de realizar el escaneo, deberá continuar con la selección. Puede configurar el código fuente en la vista Propiedades o con el Asistente de proyecto nuevo. Este capítulo le muestra cómo utilizar el asistente. Consulte “Vista Propiedades” en la página 296 para ver una visión general de las propiedades de aplicaciones y proyectos.

AppScan Source for Analysis utiliza un modelo de proyecto/aplicación que importa directamente proyectos de Microsoft Visual Studio, Eclipse, Rational Application Developer for WebSphere Software (RAD) o AppScan Source creados con anterioridad con los programas de utilidad de AppScan Source (consulte *IBM Security AppScan Source Utilities Guía del usuario* para obtener más detalles).

Puede añadir y configurar proyectos de varios tipos y que contengan diversos lenguajes, especificando valores obtenidos del código base de destino y sus procedimientos de creación. Durante la configuración, puede especificar directorios y archivos para excluirlos de un escaneo.

Antes de realizar el escaneo, debe configurar *aplicaciones y proyectos*. Una aplicación constituye un contenedor de proyectos; un proyecto es un conjunto de archivos que se van a escanear y los valores (configuración) utilizados.

---

### Archivos de aplicación y de proyecto de AppScan Source

Las aplicaciones y proyectos de AppScan Source tienen archivos correspondientes que mantienen la información de configuración requerida para escanear así como de personalización de la selección. Se recomienda que estos archivos residan en el mismo directorio que el código fuente, ya que la información de configuración (dependencias, opciones del compilador, etc.) obligatoria para construir los proyectos es muy similar a la obligatoria para que AppScan Source los escanee satisfactoriamente. Una práctica recomendada incluye gestionar estos archivos con su sistema de control de origen.

Las aplicaciones y los proyectos creados en AppScan Source for Analysis tienen una extensión .paf y .ppf, respectivamente. Estos archivos se generan cuando se crea y configura manualmente una aplicación o proyecto en AppScan Source for Analysis, AppScan Source for Automation y en la AppScan Source.

En Windows, cuando importa soluciones y proyectos de Visual Studio en AppScan Source for Analysis, AppScan Source for Automation y la AppScan Source, se crean para estas soluciones y proyectos archivos con extensiones .sln.gaf y .vcproj.gpf.

En macOS, cuando importa directorios y proyectos Xcode, se crean para los mismos archivos con las extensiones `.xcodeproj.gaf` y `.xcodeproj.gpf`. Del mismo modo cuando importa un espacio de trabajo Xcode, se crea un archivo con una extensión `.xcworkspace.gaf`.

**Nota:** Cuando un Importador de Eclipse se ejecuta en Eclipse o en un espacio de trabajo de Rational Application Developer for WebSphere Software (RAD), AppScan Source crea archivos intermedios con extensiones `.ewf` y `.epf`. Estos archivos son necesarios para la importación inicial en AppScan Source for Analysis y para futuros escaneos.

**Importante:** Si está trabajando con un proyecto AppScan Source que tiene dependencias en un entorno de desarrollo, por ejemplo, un proyecto de IBM MobileFirst Platform, asegúrese de que crea el proyecto en el entorno de desarrollo antes de importarlo. Después de importar el proyecto, si modifica los archivos que contiene, asegúrese de que vuelve a crearlo en el entorno de desarrollo antes del escaneo en AppScan Source. Si no lo hace, AppScan Source omite las modificaciones que se realicen en los archivos.

*Tabla 2. archivos de AppScan Source*

| Extensión de archivo de AppScan Source | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ppf                                    | <ul style="list-style-type: none"> <li>• Archivo de proyecto de AppScan Source</li> <li>• Se generará cuando se cree un proyecto con AppScan Source for Analysis o con programas de utilidad soportados de AppScan Source</li> <li>• Nombre de usuario</li> </ul>                                                                                                                                                                               |
| paf                                    | <ul style="list-style-type: none"> <li>• Archivo de aplicación de AppScan Source</li> <li>• Se generará cuando se cree una aplicación con AppScan Source for Analysis o con programas de utilidad soportados de AppScan Source</li> <li>• Nombre de usuario</li> </ul>                                                                                                                                                                          |
| sln.gaf                                | <ul style="list-style-type: none"> <li>• Archivo de aplicación de AppScan Source que se genera al importar soluciones de Visual Studio</li> <li>• Utilizado para albergar información de aplicación personalizada como las exclusiones y los paquetes</li> <li>• Adopta el nombre de la solución o del espacio de trabajo importado. Por ejemplo:<br/> <code>d:\my_apps\myapp.sln</code><br/> <code>d:\my_apps\myapp.sln.gaf</code> </li> </ul> |

Tabla 2. archivos de AppScan Source (continuación)

| Extensión de archivo de AppScan Source | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vcproj.gpf                             | <ul style="list-style-type: none"> <li>• Archivo de proyecto de AppScan Source que se genera al importar proyectos de Visual Studio</li> <li>• Utilizado para albergar información de proyecto personalizada como los patrones y las exclusiones</li> <li>• Adopta el nombre del proyecto importado. Por ejemplo:<br/>d:\my_projects\myproject.vcproj<br/>d:\my_projects\myproject.vcproj.gpf</li> </ul>                              |
| xcodeproj.gaf                          | <ul style="list-style-type: none"> <li>• El archivo de aplicación de AppScan Source que se genera al importar directorios Xcode</li> <li>• Utilizado para albergar información de aplicación personalizada como las exclusiones y los paquetes</li> <li>• Adopta el nombre de la solución o del espacio de trabajo importado. Por ejemplo:<br/>/Users/myUser/myProject.xcodeproj<br/>/Users/myUser/myProject.xcodeproj.gaf</li> </ul> |
| xcodeproj.gpf                          | <ul style="list-style-type: none"> <li>• El archivo de proyecto de AppScan Source que se genera al importar directorios Xcode</li> <li>• Utilizado para albergar información de proyecto personalizada como los patrones y las exclusiones</li> <li>• Adopta el nombre del proyecto importado: Por ejemplo:<br/>/Users/myUser/myProject.xcodeproj<br/>/Users/myUser/myProject.xcodeproj.gpf</li> </ul>                                |
| xcworkspace.gaf                        | <ul style="list-style-type: none"> <li>• El archivo de aplicación de AppScan Source que se genera cuando importa un espacio de trabajo de Xcode.</li> <li>• Utilizado para albergar información de aplicación personalizada como las exclusiones y los paquetes</li> <li>• Adopta el nombre del espacio de trabajo importado. Por ejemplo:<br/>/Users/myUser/myProj.xcworkspace.gaf</li> </ul>                                        |

Tabla 2. archivos de AppScan Source (continuación)

| Extensión de archivo de AppScan Source | Descripción                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ewf                                    | <ul style="list-style-type: none"> <li>• Archivo del espacio de trabajo de Eclipse</li> <li>• Se produce cuando se importa un espacio de trabajo de Eclipse en AppScan Source</li> <li>• El exportador de Eclipse crea el archivo según la información del espacio de trabajo de Eclipse - AppScan Source importará entonces el archivo</li> </ul> |
| epf                                    | <ul style="list-style-type: none"> <li>• Archivo de proyecto de Eclipse</li> <li>• Se produce cuando un proyecto de Eclipse se importa en AppScan Source</li> <li>• El exportador de Eclipse crea el archivo según la información del proyecto de Eclipse - AppScan Source importará entonces el archivo</li> </ul>                                |

**Consejo:** Cuando utiliza las herramientas de integración de compilación (por ejemplo, Ounce/Ant o Ounce/Maven) para generar archivos de proyectos y aplicaciones AppScan Source, se recomienda actualizar estos archivos en el control de origen como parte de su automatización de compilación para facilitar su compartición con todo equipo de desarrollo. Cuando un desarrollador actualice la vista local de los archivos del control de origen, la aplicación de AppScan Source y los archivos de proyecto también se actualizarán. Esto asegura que todo el equipo esté trabajando con un conjunto de archivos coherente.

**Nota:** Para conocer a qué versiones de archivos importados da soporte AppScan Source for Analysis, AppScan Source for Automation y la AppScan Source, consulte <http://www.ibm.com/support/docview.wss?uid=swg27027486>. En esta página, seleccione el separador de la versión de AppScan Source que está utilizando y, a continuación, seleccione el componente de AppScan Source que está utilizando. Si AppScan Source da soporte a la apertura y escando de archivos desde otros entornos de desarrollo, este soporte se muestra en la sección **Compiladores y lenguajes del separador Software soportado**.

## Configuración de aplicaciones

Puede utilizar el Asistente para aplicaciones nuevas o Application Discovery Assistant para crear aplicaciones. Application Discovery Assistant automatiza la configuración de la aplicación, mientras que el asistente para aplicaciones nuevas le permite añadir aplicaciones y le guía por el proceso de configuración. El asistente le ayuda a crear manualmente un proyecto o a añadir proyectos existentes a una aplicación. En este apartado se describen estos dos métodos para añadir aplicaciones y tareas de configuración básicas.

**Nota:** Application Discovery Assistant crea y configura con rapidez aplicaciones o proyectos para código fuente Java y soluciones Microsoft Visual Studio - o Eclipse o espacios de trabajo de IBM Rational Application Developer for WebSphere Software (RAD) que contienen proyectos Java. Para crear una aplicación para cualquier otro lenguaje soportado, utilice el Asistente Nueva aplicación o importe aplicaciones soportadas en AppScan Source for Analysis.

Debe crear una aplicación nueva (consulte “Creación de una nueva aplicación con el Asistente para aplicaciones nuevas” o “Utilización de Application Discovery Assistant para crear aplicaciones y proyectos” en la página 38) o añadir una aplicación existente (consulte “Adición de una aplicación existente” en la página 41) antes de añadir proyectos. Si utiliza Microsoft Visual Studio, los archivos de origen ya se organizan en proyectos. AppScan Source for Analysis permite importar soluciones y tratarlas como aplicaciones de AppScan Source.

La tabla siguiente contiene los tipos de archivos de aplicación que puede abrir y escanear con AppScan Source for Analysis.

*Tabla 3. Tipos de archivos de aplicación soportados*

| Aplicación                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Tipo de archivo                                                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Microsoft Visual Studio<br><b>Nota:</b> Para conocer a qué versiones de archivos importados da soporte AppScan Source for Analysis, AppScan Source for Automation y la AppScan Source, consulte <a href="http://www.ibm.com/support/docview.wss?uid=swg27027486">http://www.ibm.com/support/docview.wss?uid=swg27027486</a> . En esta página, seleccione el separador de la versión de AppScan Source que está utilizando y, a continuación, seleccione el componente de AppScan Source que está utilizando. Si AppScan Source da soporte a la apertura y escando de archivos desde otros entornos de desarrollo, este soporte se muestra en la sección <b>Compiladores y lenguajes</b> del separador <b>Software soportado</b> . | Directorio .sln (Solución)                                                                                                                |
| <ul style="list-style-type: none"> <li>• Espacio de trabajo de Eclipse (sólo para Java)</li> <li>• Espacio de trabajo de RAD (sólo para Java)</li> </ul> <p>Consulte los requisitos del sistema AppScan Source para conocer las versiones de Eclipse y RAD soportadas para el escaneo del espacio de trabajo.</p>                                                                                                                                                                                                                                                                                                                                                                                                                 | <p>&lt;directorio espacio_trabajo&gt; o .ewf</p> <p>El directorio del espacio de trabajo contiene un directorio adicional, .metadata.</p> |
| Archivo de aplicación de AppScan Source                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | .paf                                                                                                                                      |

**Consejo:** Aparece un icono en la vista Explorador que indica una aplicación importada (consulte “Indicadores de aplicaciones y proyectos” en la página 90).

**Nota:** Si las aplicaciones y proyectos se crean utilizando el Asistente para aplicaciones nuevas y el Asistente de proyecto nuevo, el nombre de archivo se asigna automáticamente de acuerdo con el **Nombre** especificado en el asistente (por ejemplo, si un proyecto se crea y se especifica **MyProject** en el campo **Nombre**, el nombre de archivo del proyecto será **MyProject.ppf**). Se pueden cambiar los nombres de aplicaciones y proyectos utilizando la vista Propiedades.

## Creación de una nueva aplicación con el Asistente para aplicaciones nuevas

### Procedimiento

1. Realice una de estas acciones:

- Seleccione **Archivo > Añadir aplicación > Crear una nueva aplicación** en la barra del menú principal.
  - En la barra de herramientas de la vista Explorador, pulse el botón de flecha hacia abajo **Añadir menú de aplicación** y seleccione **Crear una nueva aplicación** en el menú.
  - En la vista Explorador, pulse con el botón derecho **Todas las aplicaciones** y luego seleccione **Añadir aplicación > Crear una nueva aplicación** en el menú.
2. Escriba un **Nombre** para la aplicación.
  3. Vaya al **Directorio de trabajo** en el que desea guardar la aplicación. La extensión del nombre de archivo de la nueva aplicación será **.paf**.
  4. Pulse **Siguiente** para configurar los proyectos que comprenden la aplicación o **Finalizar** para añadir la aplicación sin configurar ningún proyecto. Puede encontrar ayuda para configurar y añadir proyectos más adelante en esta sección.

## Utilización de Application Discovery Assistant para crear aplicaciones y proyectos

AppScan Source incluye un potente Application Discovery Assistant que permite crear y configurar con rapidez aplicaciones y proyectos para código fuente Java y soluciones Microsoft Visual Studio. Application Discovery Assistant también le permite localizar espacios de trabajo Eclipse o Rational Application Developer for WebSphere Software (RAD) que contienen proyectos Java. Application Discovery Assistant permite apuntar a su código fuente, solución o directorio de espacio de trabajo y, a continuación AppScan Source maneja el resto.

### Acerca de esta tarea

Utilice Application Discovery Assistant para buscar una ubicación que contenga una combinación de código fuente Java, soluciones de Microsoft Visual Studio y/o espacios de trabajo de Eclipse. El último panel de Application Discovery Assistant permite especificar preferencias de estructura de aplicación/proyecto sólo para Java. Este panel no influye en la ubicación de los archivos de proyecto y aplicación para la solución de Microsoft Visual Studio o espacios de trabajo de Eclipse, donde los archivos de aplicación se colocan de forma automática en la raíz de la solución o del espacio de trabajo, y los archivos de proyecto se colocan de forma automática en la raíz de la solución o los proyectos de espacio de trabajo.

### Procedimiento

1. Realice una de estas acciones para iniciar Application Discovery Assistant:
  - Seleccione **Archivo > Añadir aplicación > Descubrir aplicaciones** en la barra del menú principal.
  - En la vista Explorador, seleccione la sección **Inicio rápido y Descubrir aplicaciones**.
  - En la barra de herramientas de la vista Explorador, pulse el botón de flecha hacia abajo **Añadir menú de aplicación** y seleccione **Descubrir aplicaciones** en el menú.
  - En la vista Explorador, pulse con el botón derecho **Todas las aplicaciones** y luego seleccione **Añadir aplicación > Descubrir aplicaciones** en el menú.
2. En el panel Ubicación de búsqueda, especifique la ubicación que contiene el código fuente, las soluciones o los espacios de trabajo que desea escanear.

Asimismo, puede establecer el escaneo para que empiece inmediatamente después de completar el descubrimiento de aplicaciones.

A partir de aquí, puede pulsar **Siguiente** para establecer las opciones adicionales de Application Discovery Assistant (por ejemplo, la especificación de dependencias externas, las reglas de exclusión y las preferencias de estructura de proyecto/aplicación de Java), o puede pulsar **Iniciar** para empezar el descubrimiento de aplicaciones. Si pulsa **Iniciar**:

- No se establecerán ubicaciones de dependencias externas. Si la aplicación tiene dependencias externas y no se especifican, los resultados del escaneo se verán afectados negativamente.
- Se utilizarán las reglas de exclusión de uso inmediato (consulte “Reglas de exclusión predeterminadas de Application Discovery Assistant” en la página 41 para obtener una lista de las reglas predeterminadas).
- Si localiza código fuente de Java, se crearán un proyecto y una aplicación (el proyecto individual contendrá todas las raíces de origen que se encuentren).

Si pulsa **Siguiente**, continúe en el paso siguiente.

3. En el panel Dependencias externas, establezca una vía de acceso para cada dependencia externa que tenga la aplicación (por ejemplo, una vía de acceso a un JDK o un servidor web). Para completar el panel, siga estas instrucciones:
  - a. Para añadir una dependencia externa, pulse dentro de la tabla o pulse **Añadir** y, a continuación, escriba o busque la vía de acceso de la dependencia externa. Para aceptar una vía de acceso que ha especificado mediante el teclado, pulse la tecla Intro.

**Consejo:** Si escribe en el campo de vía de acceso de la dependencia mientras se está editando, aparecen directorios que puede seleccionar. Debe escribir como mínimo una letra de unidad. Para la vía de acceso especificada, se mostrarán todas las carpetas que contenga.

- b. Para eliminar una vía de acceso de dependencia externa, selecciónela y pulse **Suprimir**.
- c. Para modificar una vía de acceso de dependencia externa, pulse dentro de la vía de acceso y, a continuación, escriba o busque la vía de acceso de la dependencia externa.

A partir de aquí, puede pulsar **Siguiente** para establecer las opciones adicionales de Application Discovery Assistant, o puede pulsar **Iniciar** para empezar el descubrimiento de aplicaciones. Si pulsa **Iniciar**:

- Se utilizarán las reglas de exclusión de uso inmediato (consulte “Reglas de exclusión predeterminadas de Application Discovery Assistant” en la página 41 para obtener una lista de las reglas predeterminadas).
- Si localiza código fuente de Java, se crearán un proyecto y una aplicación (el proyecto individual contendrá todas las raíces de origen que se encuentren).

Si pulsa **Siguiente**, continúe en el paso siguiente.

4. En el panel Reglas de exclusión, especifique las reglas para filtrar los archivos y los directorios. Las reglas se establecen por expresión regular de PERL, Grep, EGrep o coincidencia exacta. Por ejemplo, si desea excluir un directorio denominado temp de la búsqueda de Application Discovery, puede añadir una regla de exclusión PERL `.*[\\/]temp`.

De forma predeterminada, se proporciona un conjunto de expresiones regulares de PERL para excluir algunos directorios comunes (consulte “Reglas de exclusión predeterminadas de Application Discovery Assistant” en la página 41 para obtener la lista completa). Para modificar esta lista o crear reglas nuevas, siga estas instrucciones:

- a. Para modificar una regla de exclusión existente, pulse dentro de la regla para activar el editor de reglas. Cuando haya terminado de editar la regla, pulse fuera de ella o pulse la tecla **Intro** del teclado.  
Para modificar el tipo de expresión regular de una regla existente, pulse dentro de la celda **Tipo de expresión regular** de la regla y, a continuación, seleccione el tipo de expresión regular en el menú.
- b. Para añadir una regla de exclusión, pulse **Añadir**. Se añade una regla nueva a la tabla, que puede alterar siguiendo las instrucciones anteriores para modificar reglas.
- c. Para eliminar una regla de exclusión, selecciónela y pulse **Suprimir** (o pulse **Suprimir todo** para eliminar todas las reglas de exclusión que aparecen actualmente en el panel).

**Importante:** Las reglas de exclusión válidas se denotan con una marca de selección en la tabla; las reglas no válidas se denotan con una X roja. No podrá iniciar el Application Discovery o continuar en Application Discovery Assistant hasta que todas las reglas sean válidas.

A partir de aquí:

- Si sólo busca código fuente de Java, puede pulsar **Siguiente** para establecer las preferencias de estructura de proyecto/aplicación de Application Discovery Assistant, o puede pulsar **Iniciar** para ejecutar el asistente.
- Si sólo busca soluciones de Microsoft Visual Studio o espacios de trabajo de Eclipse, pulse **Iniciar** para ejecutar el asistente. Si pulsa **Siguiente**, el asistente continuará en un panel que sólo se aplica al descubrimiento de código fuente de Java.

Si pulsa **Siguiente**, continúe en el paso siguiente.

5. El panel Creación de la aplicación y el proyecto sólo se aplica al descubrimiento de código fuente de Java. En él, especifique la estructura de las aplicaciones y los proyectos que se crearán:
  - a. Para crear un proyecto individual para todas las raíces de origen que se detecten, seleccione **Crear un solo proyecto** en el menú **Proyectos**. Con esta selección, únicamente tendrá la opción de crear una aplicación individual.
  - b. Para crear un proyecto aparte para cada raíz de origen que se detecte, seleccione **Crear un proyecto para cada raíz de origen encontrada** en el menú **Proyectos**. Con esta selección, puede crear una aplicación o varias aplicaciones. Para crear una sola aplicación que contenga todos los proyectos que se creen, seleccione **Crear una sola aplicación** en el menú **Aplicaciones**. Para crear una aplicación para cada proyecto que se cree, seleccione **Crear una aplicación por proyecto** en el menú **Aplicaciones**.

Asimismo, seleccione una ubicación para almacenar los archivos de definición de proyectos y aplicaciones.

Si elige **Organizar los archivos en mi nombre**:

- Si está creando un proyecto individual, los archivos de proyecto y aplicación se crearán en la ubicación de búsqueda.
- Si está creando un proyecto para cada raíz de origen en una aplicación individual, el archivo de proyecto de cada raíz de origen se creará en el directorio superior a la raíz del origen y el archivo de aplicación se creará en la ubicación de búsqueda.
- Si está creando un proyecto para cada raíz de origen y una aplicación para cada proyecto, los archivos de proyecto y aplicación de cada raíz de origen se crearán en el directorio superior a la raíz del origen.



Si especifica un directorio, todos los archivos de proyecto y aplicación se crearán en ese directorio.

6. Si desea cambiar alguno de los valores establecidos en los paneles anteriores, pulse **Atrás**. Si está satisfecho con los valores de Application Discovery, pulse **Iniciar** para escanear la ubicación de búsqueda en busca de raíces de origen.

## Resultados

Cuando el Application Discovery haya finalizado, las nuevas aplicaciones y los nuevos proyectos que se han creado como resultado del Application Discovery aparecerán en la vista Explorador, preparados para el escaneo (si ha establecido el escaneo para que se inicie inmediatamente después de completar el descubrimiento de aplicaciones, se iniciará el escaneo).

Si se han encontrado problemas durante el descubrimiento, Application Discovery Assistant proporciona un informe de descubrimiento al finalizar. Por ejemplo, si la aplicación tiene dependencias externas que no se han especificado en el panel Dependencias externas, el informe contendrá avisos indicando que las dependencias externas no pueden resolverse. En el informe de descubrimiento:

- Pulse **Finalizar** para crear las aplicaciones y los proyectos. Si selecciona **Ignorar avisos y escanear de cualquier modo**, las aplicaciones y proyectos se escanearán inmediatamente.
- Pulse **Atrás** para modificar los valores de Application Discovery Assistant o ejecutar el Application Discovery de nuevo.
- Pulse **Cancelar** para cerrar el informe de descubrimiento sin crear aplicaciones o proyectos.

## Reglas de exclusión predeterminadas de Application Discovery Assistant

Cuando se utiliza Application Discovery Assistant, se utilizan las reglas de exclusión predeterminadas si el panel Reglas de exclusión no se modifica, o si inicia el Application Discovery después de especificar un directorio de búsqueda. En este tema se describen las reglas de exclusión predeterminadas del Application Discovery.

Tabla 4. Reglas de exclusión predeterminadas de Application Discovery

| Regla de exclusión | Tipo de expresión regular |
|--------------------|---------------------------|
| .*[\\/]example     | PERL                      |
| .*[\\/]test        | PERL                      |
| .*[\\/]demo        | PERL                      |
| .*[\\/]sample      | PERL                      |

## Adición de una aplicación existente

Las aplicaciones existentes se pueden añadir al escaneo arrastrándolas y soltándolas en la vista Explorador o mediante la acción **Añadir aplicación**. Además, se pueden añadir los archivos WAR y EAR arrastrándolos y soltándolos en la vista Explorador.

Para obtener información acerca de cómo añadir una aplicación, consulte estos temas:

- “Adición de una aplicación existente con acciones de la interfaz de usuario” en la página 42

- “Adición de una aplicación existente con arrastrar y soltar”

## Adición de una aplicación existente con acciones de la interfaz de usuario

### Procedimiento

1. Realice una de estas acciones:
  - Seleccione **Archivo > Añadir aplicación > Abrir una aplicación existente** en el menú principal del espacio de trabajo.
  - En la barra de herramientas de la vista Explorador, pulse el botón de flecha hacia abajo **Añadir menú de aplicación** y seleccione **Abrir una aplicación existente** en el menú.
  - En la vista Explorador, pulse con el botón derecho **Todas las aplicaciones** y luego seleccione **Añadir aplicación > Abrir una aplicación existente** en el menú.
2. Seleccione el directorio que contiene el archivo de aplicación que ha guardado (.paf, .sln, .dsw, o .ewf).

**Nota:** Para conocer a qué versiones de archivos importados da soporte AppScan Source for Analysis, AppScan Source for Automation y la AppScan Source, consulte <http://www.ibm.com/support/docview.wss?uid=swg27027486>. En esta página, seleccione el separador de la versión de AppScan Source que está utilizando y, a continuación, seleccione el componente de AppScan Source que está utilizando. Si AppScan Source da soporte a la apertura y escando de archivos desde otros entornos de desarrollo, este soporte se muestra en la sección **Compiladores y lenguajes** del separador **Software soportado**.

3. Abra el archivo de la aplicación.

## Adición de una aplicación existente con arrastrar y soltar

### Procedimiento

1. En la estación de trabajo, localice la aplicación (.paf, .war, .ear, .sln, .dsw, o .ewf) que desee añadir para escanear. También puede añadir un directorio que contenga archivos .war o .ear (en algunos servidores de aplicaciones, éstos se llaman *carpetas de arrastre*).

**Nota:** No puede arrastrar y soltar directorios del espacio de trabajo de Eclipse.

**Nota:** Si está añadiendo un archivo .war o .ear, o un directorio que contenga archivos .war o .ear, los archivos deben estar en el sistema de archivos local o en unidad correlacionada.

**Nota:** Para conocer a qué versiones de archivos importados da soporte AppScan Source for Analysis, AppScan Source for Automation y la AppScan Source, consulte <http://www.ibm.com/support/docview.wss?uid=swg27027486>. En esta página, seleccione el separador de la versión de AppScan Source que está utilizando y, a continuación, seleccione el componente de AppScan Source que está utilizando. Si AppScan Source da soporte a la apertura y escando de archivos desde otros entornos de desarrollo, este soporte se muestra en la sección **Compiladores y lenguajes** del separador **Software soportado**.

2. Seleccione la aplicación y luego arrástrela a la vista Explorador.
3. Suelte la selección en el nodo **Todas las aplicaciones** o bajo el mismo.

4. Si está añadiendo un archivo .war o .ear, o un directorio que contenga archivos .war o .ear, se abrirá un recuadro de diálogo que le permitirá especificar el servidor de aplicaciones en el que está desplegado el archivo o archivos. Pulse **Aceptar** tras completar el recuadro de diálogo.

## Adición de varias aplicaciones

En lugar de añadir las aplicaciones de una en una, es posible que cuando empiece a trabajar con AppScan Source for Analysis, puede desear importar varias aplicaciones. El recuadro de diálogo Seleccionar aplicaciones le permite seleccionar el directorio raíz en el que buscar aplicaciones de AppScan Source (.paf) o archivos de soluciones de Visual Studio (.sln). También se pueden añadir varias aplicaciones para escaneo arrastrándolas y soltándolas en la vista Explorador.

Para obtener información acerca de cómo añadir varias aplicaciones, consulte estos temas:

- “Adición de varias aplicaciones con acciones de la interfaz de usuario”
- “Adición de varias aplicaciones con arrastrar y soltar”

**Nota:** Para añadir varios archivos WAR y EAR, lo puede hacer arrastrando y soltando un directorio que contenga los archivos. Para obtener más información, consulte “Adición de una aplicación existente con arrastrar y soltar” en la página 42.

### Adición de varias aplicaciones con acciones de la interfaz de usuario

#### Procedimiento

1. Seleccione **Archivo > Añadir aplicación > Varias aplicaciones** en el menú principal del espacio de trabajo.
2. En el cuadro de diálogo Seleccionar aplicaciones, vaya al directorio raíz que contiene las aplicaciones que desea importar. Marque el cuadro de selección **Realizar recursividad en subdirectorios** para buscar en subdirectorios.
3. Realice una de estas acciones:
  - Pulse **Finalizar** para importar las aplicaciones y añadirlas a la vista Explorador.
  - Pulse **Siguiente** para ver los resultados de la búsqueda y seleccionar las aplicaciones que se han de añadir. Luego pulse **Finalizar**.

**Nota:** Para conocer a qué versiones de archivos importados da soporte AppScan Source for Analysis, AppScan Source for Automation y la AppScan Source, consulte <http://www.ibm.com/support/docview.wss?uid=swg27027486>. En esta página, seleccione el separador de la versión de AppScan Source que está utilizando y, a continuación, seleccione el componente de AppScan Source que está utilizando. Si AppScan Source da soporte a la apertura y escando de archivos desde otros entornos de desarrollo, este soporte se muestra en la sección **Compiladores y lenguajes** del separador **Software soportado**.

### Adición de varias aplicaciones con arrastrar y soltar

#### Procedimiento

1. En su estación de trabajo, localice las aplicaciones (archivos .paf, .sln, .dsw o .ewf) que desee añadir para escanear.

**Nota:** No puede arrastrar y soltar directorios del espacio de trabajo de Eclipse.

**Nota:** Para conocer a qué versiones de archivos importados da soporte AppScan Source for Analysis, AppScan Source for Automation y la AppScan Source, consulte <http://www.ibm.com/support/docview.wss?uid=swg27027486>. En esta página, seleccione el separador de la versión de AppScan Source que está utilizando y, a continuación, seleccione el componente de AppScan Source que está utilizando. Si AppScan Source da soporte a la apertura y escando de archivos desde otros entornos de desarrollo, este soporte se muestra en la sección **Compiladores y lenguajes** del separador **Software soportado**.

2. Seleccione una o varias aplicaciones y arrástrelas a la vista Explorador.
3. Suelte la selección en el nodo **Todas las aplicaciones** o bajo el mismo.

## Importación de las aplicaciones Java desde Apache Tomcat y los servidores de aplicaciones de WebSphere Application Server Liberty Profile

Si dispone de aplicaciones Java que se han desplegado en un servidor de aplicaciones soportado, puede importarlas automáticamente a AppScan Source.

### Antes de empezar

Para obtener información acerca de las versiones de Apache Tomcat y WebSphere Application Server Liberty Profile soportadas, consulte la sección Requisitos del sistema AppScan Source. En esta página seleccione el separador de la versión de AppScan Source que está utilizando y, a continuación, seleccione el componente AppScan Source for Analysis. Puede encontrar los servidores de aplicaciones soportados en la sección **Software soportado**.

### Procedimiento

1. Realice una de estas acciones:
  - Seleccione **Archivo > Añadir aplicación > Importar desde un servidor de aplicaciones** en el menú del espacio de trabajo principal.
  - En la barra de herramientas de la vista Explorador, pulse el botón de flecha abajo de **Añadir menú de aplicación** y seleccione **Importar desde un servidor de aplicaciones**.
  - En la vista Explorador, pulse con el botón derecho **Todas las aplicaciones**, seleccione **Añadir aplicación > Importar desde un servidor de aplicaciones** desde el menú.
2. En el recuadro de diálogo Importar desde un servidor de aplicaciones, pulse **Examinar** para buscar y seleccionar la ubicación en la que está instalado el servidor de aplicaciones, o especifique la vía de acceso del servidor y el directorio en el campo y pulse **Buscar** para buscar las aplicaciones de la ubicación especificada. Si la ubicación se reconoce como un servidor de aplicaciones soportado, se listan las aplicaciones disponibles en la sección **Aplicaciones para importar** del recuadro de diálogo. En esta sección, seleccione las aplicaciones que desea importar y, a continuación, pulse **Aceptar**.
3. Se crea una aplicación de AppScan Source para cada aplicación importada desde el servidor de aplicaciones.

### Resultados

Si está importando desde un servidor de WebSphere Application Server Liberty Profile (WebSphere Application Server Versión 8.5 y superior), es posible que vea un mensaje que le indique que es necesario realizar manualmente una

precompilación del JSP. Esto es debido a que el servidor de Liberty Profile no incluye un compilador JSP autónomo. Si se muestra este mensaje, suprima cualquier aplicación que se haya creado debido a la importación y, a continuación, siga las instrucciones de la sección “Generación de JSP (JavaServer Pages) precompilado para un WebSphere Application Server Liberty Profile” y vuelva a realizar la importación desde el servidor de aplicaciones.

Cuando se importa la aplicación, de manera predeterminada, AppScan Source solo escanea sus archivos JSP y el contenido de web-inf/classes. El contenido de web-inf/lib no se escanea. Si quiere que se escaneen otros archivos, puede utilizar las propiedades del proyecto para definir otras extensiones de archivos que se deban escanear (consulte “Extensiones de archivo” en la página 261). Por ejemplo, si quiere que se escaneen archivos .jar (incluidos los que se encuentren en web-inf/lib), siga las instrucciones para modificar las propiedades del proyecto de “Modificación de las propiedades del proyecto y de la aplicación” en la página 83. En la vista Propiedades del proyecto, seleccione el separador “Extensiones de archivo” en la página 261. En la sección Extensiones adicionales de la vista, pulse **Añadir extensión**. En el recuadro de diálogo Nuevas extensiones, escriba jar en el campo **Extensión**, seleccione **Escanear archivos con esta extensión** y pulse **Aceptar**. Pulse **Guardar** en la parte superior derecha de la vista (o seleccione **Archivo > Guardar** en el menú principal) y, a continuación, escanee el proyecto de nuevo. Si hay archivos que no quiera escanear, puede excluirlos utilizando el separador de la Vista de proyecto “Orígenes” en la página 262.

Si las aplicaciones del servidor cambian y desea renovar las aplicaciones de AppScan Source con los contenidos modificados, debe volver a realizar los pasos. No es necesario que suprima, en primer lugar, las aplicaciones creadas originalmente, AppScan Source las suprimirá automáticamente después de que se vuelvan a importar.

**Nota:** Si importa un archivo .war desde un servidor y más tarde importa otro archivo .war con el mismo nombre desde otro servidor, el segundo archivo .war sobrescribirá al primero. Para evitarlo, cambie el nombre al segundo archivo .war antes de importarlo.

## Generación de JSP (JavaServer Pages) precompilado para un WebSphere Application Server Liberty Profile

Si está importando aplicaciones desde un WebSphere Application Server Liberty Profile (WebSphere Application Server Versión 8.5 y superior), es necesario que realice manualmente una precompilación del JSP, ya que Liberty Profile no incluye un compilador JSP autónomo. En este tema se describen los pasos necesarios para configurar manualmente la precompilación JSP.

### Procedimiento

1. Siga las instrucciones para crear un servidor de Liberty Profile en WebSphere Application Server Network Deployment Knowledge Center. Para WebSphere Application Server Versión 8.5.5, consulte el tema Creación de un servidor de Liberty Profile mediante las herramientas del desarrollador.
2. En el archivo server.xml de Liberty Profile, añada lo siguiente a la sección server description:

```
<jspEngine prepareJSPs="0"/>
<webContainer deferServletLoad="false"/>
```

Por ejemplo:

```

<server description="new server">

    <!-- Enable features -->
    <featureManager>
        <feature>jsp-2.2</feature>
        <feature>localConnector-1.0</feature>
        <feature>appSecurity-2.0</feature>
        <feature>restConnector-1.0</feature>
    </featureManager>

    <!-- To access this server from a remote client
         add a host attribute to the following element,
         e.g. host="*" -->
    <httpEndpoint httpPort="9080" httpsPort="9443" id="defaultHttpEndpoint"/>

    ...
    <jspEngine prepareJSPs="0"/>
    <webContainer deferServletLoad="false"/>
    ...
</server>

```

El archivo server.xml se describe en WebSphere Application Server Center. Para WebSphere Application Server Versión 8.5.5, consulte el tema Liberty Profile: Configuración de elementos en el archivo server.xml.

3. Inicie el servidor en modalidad de depuración, utilizando uno de estos métodos:
  - Añada un argumento de la JVM `-Dwas.debug.mode=true`, como se describe en la sección Configuración de argumentos en WebSphere Application Server V8.5 Liberty Profile.
  - Siga las instrucciones para iniciar y detener un servidor en WebSphere Application Server Network Deployment Knowledge Center. Para WebSphere Application Server Versión 8.5.5, consulte Inicio y detención utilizando las herramientas del desarrollador.

## Resultados

Una vez realizados estos pasos, importe sus aplicaciones Java desde WebSphere Application Server Liberty Profile realizando los pasos de la sección “Importación de las aplicaciones Java desde Apache Tomcat y los servidores de aplicaciones de WebSphere Application Server Liberty Profile” en la página 44.

## Adición de un espacio de trabajo de Eclipse o de un producto basado en Eclipse

Si tiene un espacio de trabajo de Eclipse o de Rational Application Developer for WebSphere Software (RAD) que contiene proyectos Java o proyectos IBM MobileFirst Platform, puede importarlo a AppScan Source for Analysis.

### Antes de empezar

Antes de añadir el espacio de trabajo, asegúrese de haber instalado y actualizado el entorno de desarrollo tal como se describe en “Configuración del entorno de desarrollo para proyectos de Eclipse y Rational Application Developer for WebSphere Software (RAD)” en la página 47.

### Procedimiento

1. Realice una de estas acciones:
  - Seleccione **Archivo > Añadir aplicación > Importar un espacio de trabajo basado en Eclipse existente** en el menú principal del espacio de trabajo.

- En la barra de herramientas de la vista del Explorador, pulse el botón de flecha abajo de **Añadir menú de aplicación** y seleccione **Importar un espacio de trabajo basado en Eclipse existente** en el menú.
  - En la vista del Explorador, pulse con el botón derecho **Todas las aplicaciones** y luego seleccione **Añadir aplicación > Importar un espacio de trabajo basado en Eclipse existente** en el menú.
2. Seleccione el **Tipo de espacio de trabajo**:
  3. Vaya al espacio de trabajo, seleccione el directorio y, a continuación, pulse **Aceptar** para añadir el espacio de trabajo.

---

## Configuración del entorno de desarrollo para proyectos de Eclipse y Rational Application Developer for WebSphere Software (RAD)

Antes de importar un proyecto Eclipse o Rational Application Developer for WebSphere Software (RAD), debe configurar correctamente el entorno de desarrollo. Aunque Eclipse constituye la base para cada tipo de proyecto, AppScan Source distingue entre las distintas versiones.

Para conocer a qué versiones de Eclipse y Rational Application Developer for WebSphere Software (RAD) da soporte AppScan Source, consulte <http://www.ibm.com/support/docview.wss?uid=swg27027486>.

Para obtener más información sobre cómo configurar el entorno de desarrollo, consulte estos temas de ayuda:

- “Actualizaciones de Eclipse o Application Developer”
- “Importadores del espacio de trabajo de Eclipse: configuración de preferencias de Eclipse o Rational Application Developer for WebSphere Software (RAD)” en la página 48

## Actualizaciones de Eclipse o Application Developer

Para entornos Eclipse o Application Developer externos a AppScan Source, debe asegurarse de tener instaladas las actualizaciones de software adecuadas. Estas instrucciones explican cómo obtener e instalar las actualizaciones. El procedimiento puede variar en función de la versión.

### Antes de empezar

**Importante:** AppScan Source for Development necesita un Java Runtime Environment (JRE) de la Versión 1.5 o superior. Si el entorno apunta a un JRE que no cumple con este requisito, edite el archivo `eclipse.ini` en el directorio de instalación de Eclipse para que apunte a un JRE que cumpla con este requisito. Para obtener información sobre cómo realizar este cambio en el archivo `eclipse.ini`, consulte la sección *Specifying the JVM* de <http://wiki.eclipse.org/Eclipse.ini>.

### Procedimiento

1. En el menú **Ayuda** de Eclipse, seleccione la opción para instalar software nuevo (la etiqueta del menú varía en función de la versión de Eclipse que utilice).
2. Seleccione la opción para añadir un Sitio de actualización local.
3. Cuando se le solicite la ubicación del sitio, vaya al directorio de instalación de AppScan Source.
4. Añada este sitio de actualización y siga los pasos mostrados hasta que se le solicite que reinicie Eclipse.

5. Una vez finalizada la instalación, aparece el menú de AppScan Source.

## Importadores del espacio de trabajo de Eclipse: configuración de preferencias de Eclipse o Rational Application Developer for WebSphere Software (RAD)

La instalación de AppScan Source for Analysis proporciona un importador predeterminado de Eclipse. Este importador identifica la ubicación de Eclipse y de JRE. Si el importador predeterminado de Eclipse no puede importar su espacio de trabajo, deberá crear un nuevo importador de Eclipse.

### Antes de empezar

Cada configuración de importador representa una instalación de Eclipse o Rational Application Developer for WebSphere Software (RAD). Para utilizar estas configuraciones para importar los espacios de trabajo y proyectos existentes a AppScan Source for Analysis, deberá instalar también los plug-ins de AppScan Source for Development en el entorno de Eclipse.

Antes de añadir un espacio de trabajo de RAD, debe crear una configuración para el tipo de espacio de trabajo.

### Procedimiento

1. En AppScan Source for Analysis, seleccione **Editar > Preferencias** en el menú principal del entorno de trabajo.
2. Seleccione **Importadores del espacio de trabajo de Eclipse**.
3. Pulse **Crear una nueva configuración** y, a continuación, complete el cuadro de diálogo Nueva configuración de importación para crear una configuración nueva:
  - **Producto:** seleccione el producto adecuado

**Nota:** Si el producto que se ha utilizado para crear el espacio de trabajo no está disponible para su selección, asegúrese de haber completado los pasos de configuración que se describen en “Actualizaciones de Eclipse o Application Developer” en la página 47 antes de intentar crear el importador del espacio de trabajo.

- **Nombre:** nombre del importador
  - **Ubicación:** vía de acceso al directorio base de la instalación de Eclipse
  - **Ubicación de JRE:** vía de acceso al directorio raíz de Java Runtime Environment (JRE). Utilice un JDK en <install\_dir>\JDKS (donde <dir\_instalación> es la ubicación de la instalación de AppScan Source) o cualquier otro JDK preferido.
4. Pulse en **Aceptar**.
  5. Para identificar el importador como valor predeterminado, selecciónelo y pulse **Establecer como predeterminada la configuración seleccionada**. Esto hace que se muestre un icono en la columna **Predeterminado** del importador.

---

## Creación de un nuevo proyecto para una aplicación

Después de añadir una aplicación, se añaden proyectos a la misma. Los tipos de proyecto que se pueden escanear son: Java/JSP, ASP, C/C++, COBOL, ColdFusion, .NET Assembly, Pattern Based, Perl, PHP, PL/SQL, T-SQL, Visual Basic y JavaScript.



## Acerca de esta tarea

Si utiliza make para compilar el proyecto, se recomienda utilizar el programa de utilidad Ounce/Make para crear un archivo de proyecto y luego añadir el archivo de proyecto. Si utiliza ant para compilar el proyecto, utilice Ounce/Ant para crear un archivo de proyecto y, a continuación, añada el archivo de proyecto. Consulte *IBM Rational AppScan Source Edition Utilities Guía del usuario* para obtener información detallada sobre Ounce/Make y Ounce/Ant.

**Nota:** La codificación del archivo predeterminado para proyectos AppScan Source es **ISO-8859-1**. La codificación de archivos predeterminada se puede cambiar en la página de preferencias generales.

**Nota:** Si las aplicaciones y proyectos se crean utilizando el Asistente para aplicaciones nuevas y el Asistente de proyecto nuevo, el nombre de archivo se asigna automáticamente de acuerdo con el **Nombre** especificado en el asistente (por ejemplo, si un proyecto se crea y se especifica **MyProject** en el campo **Nombre**, el nombre de archivo del proyecto será **MyProject.ppf**). Se pueden cambiar los nombres de aplicaciones y proyectos utilizando la vista Propiedades.

## Procedimiento

1. En la vista Explorador, seleccione la aplicación a la que desea añadir el proyecto (si aún no ha añadido una aplicación, consulte “Configuración de aplicaciones” en la página 36).
2. Realice una de estas acciones para abrir el Asistente de proyecto nuevo:
  - a. Seleccione **Archivo > Añadir proyecto > Proyecto nuevo** en el menú principal del espacio de trabajo.
  - b. Pulse con el botón derecho en la aplicación seleccionada y elija **Añadir proyecto > Proyecto nuevo** en el menú de contexto.
3. Complete el Asistente de proyecto nuevo.

## Adición de un proyecto existente

Puede añadir proyectos de AppScan Source (archivos .ppf) creados previamente con AppScan Source for Analysis a las aplicaciones de AppScan Source. También puede añadir archivos de proyectos de Eclipse (.epf), proyectos creados por cualquiera de las herramientas de integración de compilación soportadas (por ejemplo, Ounce/Maven o Ounce/Ant) o archivos de proyecto creados con Microsoft Visual C/C++ (.vcproj o .dsp), VB.NET (.vbproj) o C# (.csproj).

En esta tabla se muestra una lista de los tipos de archivo de proyecto que se pueden abrir y escanear con AppScan Source for Analysis:

*Tabla 5. Tipos de archivos de proyecto que puede abrir*

| Tipo de archivo de proyecto           | Extensión de archivo |
|---------------------------------------|----------------------|
| Microsoft Visual Studio (versión 6)   | .dsp                 |
| Microsoft Visual Studio C/C++         | .vcproj              |
| Microsoft Visual Studio C#            | .csproj              |
| Microsoft Visual Studio Visual Basic  | .vbproj              |
| Archivo de proyecto de AppScan Source | .ppf                 |
| Archivo de proyecto de Eclipse        | .epf                 |

Para obtener información acerca de cómo añadir un proyecto existente, consulte estos temas:

- “Adición de un proyecto existente con acciones de la interfaz de usuario”
- “Adición de un proyecto existente con arrastrar y soltar”

**Importante:** Si está trabajando con un proyecto AppScan Source que tiene dependencias en un entorno de desarrollo, por ejemplo, un proyecto de IBM MobileFirst Platform, asegúrese de que crea el proyecto en el entorno de desarrollo antes de importarlo. Después de importar el proyecto, si modifica los archivos que contiene, asegúrese de que vuelve a crearlo en el entorno de desarrollo antes del escaneo en AppScan Source. Si no lo hace, AppScan Source omite las modificaciones que se realicen en los archivos.

**Nota:** Cuando importa un proyecto .NET existente, puede especificar ensamblados adicionales para escanear. Añada estos ensamblados en la vista Propiedades del proyecto en el separador Ensamblados adicionales. Cuando añade ensamblados adicionales, puede combinar en un solo escaneo proyectos .NET compilados con ensamblados (incluidos los ensamblados de otros proveedores) que no se han compilado.

**Nota:** También puede añadir los archivos WAR y EAR arrastrándolos y soltándolos en la vista Explorador; sin embargo, éstos se añadirán como aplicaciones y no como proyectos. Para obtener más información, consulte “Adición de una aplicación existente con arrastrar y soltar” en la página 42.

## **Adición de un proyecto existente con acciones de la interfaz de usuario**

### **Procedimiento**

1. En la vista Explorador, seleccione la aplicación a la que desea añadir el proyecto (si aún no ha añadido una aplicación, consulte “Configuración de aplicaciones” en la página 36).
2. Realice una de estas acciones:
  - Seleccione **Archivo > Añadir proyecto > Proyecto existente** en el menú principal del espacio de trabajo.
  - Pulse con el botón derecho en la aplicación seleccionada y seleccione **Añadir proyecto > Proyecto existente** en el menú de contexto.
3. Vaya al archivo del proyecto para añadirlo a la aplicación.

**Importante:** Si está trabajando con un proyecto AppScan Source que tiene dependencias en un entorno de desarrollo, por ejemplo, un proyecto de IBM MobileFirst Platform, asegúrese de que crea el proyecto en el entorno de desarrollo antes de importarlo. Después de importar el proyecto, si modifica los archivos que contiene, asegúrese de que vuelve a crearlo en el entorno de desarrollo antes del escaneo en AppScan Source. Si no lo hace, AppScan Source omite las modificaciones que se realicen en los archivos.

## **Adición de un proyecto existente con arrastrar y soltar**

### **Procedimiento**

1. En la estación de trabajo, localice el directorio de proyecto (.ppf, .vcproj, .dsp, .vbproj o .csproj) que desea añadir para el escaneo.

**Nota:** No es posible arrastrar y soltar archivos creados por ninguna de las herramientas de integración de compilación soportadas (como, por ejemplo, Ounce/Maven o Ounce/Ant).

2. Seleccione el proyecto y luego arrástrelo a la vista Explorador de AppScan Source for Analysis.
3. Siga uno de estos pasos:
  - a. Suelte la selección en una aplicación existente.
  - b. Suelte la selección en el nodo **Todas las aplicaciones** o bajo el mismo. Puesto que los proyectos deben estar contenidos en una aplicación y esta sección no añade el proyecto a una aplicación existente, el Asistente para aplicaciones nuevas le solicitará que cree una nueva aplicación para el proyecto. Especifique un **Nombre** para la aplicación y vaya al **Directorio de trabajo** en el que desea guardar la aplicación. Pulse **Finalizar** para crear la nueva aplicación (en la vista Explorador, el proyecto añadido aparecerá contenido en ella).

**Importante:** Si está trabajando con un proyecto AppScan Source que tiene dependencias en un entorno de desarrollo, por ejemplo, un proyecto de IBM MobileFirst Platform, asegúrese de que crea el proyecto en el entorno de desarrollo antes de importarlo. Después de importar el proyecto, si modifica los archivos que contiene, asegúrese de que vuelve a crearlo en el entorno de desarrollo antes del escaneo en AppScan Source. Si no lo hace, AppScan Source omite las modificaciones que se realicen en los archivos.

## Adición de varios proyectos

Cuando añade varios proyectos a una aplicación, puede arrastrarlos y soltarlos en la vista Explorador o puede ir a un directorio para proyectos e importar algunos de ellos, o todos, en la aplicación actual.

Para obtener información acerca de cómo añadir varios proyectos, consulte estos temas:

- “Adición de varios proyectos con acciones de la interfaz de usuario”
- “Adición de varios proyectos con arrastrar y soltar” en la página 52

**Importante:** Si está trabajando con un proyecto AppScan Source que tiene dependencias en un entorno de desarrollo, por ejemplo, un proyecto de IBM MobileFirst Platform, asegúrese de que crea el proyecto en el entorno de desarrollo antes de importarlo. Después de importar el proyecto, si modifica los archivos que contiene, asegúrese de que vuelve a crearlo en el entorno de desarrollo antes del escaneo en AppScan Source. Si no lo hace, AppScan Source omite las modificaciones que se realicen en los archivos.

### Adición de varios proyectos con acciones de la interfaz de usuario

Se pueden añadir varios proyectos a una aplicación desde un directorio (incluidos los subdirectorios), un espacio de trabajo de Eclipse o Rational Application Developer for WebSphere Software (RAD), o desde un archivo de solución Microsoft.

### Procedimiento

1. En la vista Explorador, seleccione la aplicación a la que desea añadir los proyectos (si aún no ha añadido una aplicación, consulte “Configuración de aplicaciones” en la página 36).
2. Realice una de estas acciones:
  - Seleccione **Archivo > Añadir proyecto > Varios proyectos** en el menú principal del espacio de trabajo.

- Pulse con el botón derecho en la aplicación seleccionada y elija **Añadir proyecto > Varios proyectos** en el menú de contexto.
3. En el cuadro de diálogo **Añadir varios proyectos**, realice una de estas acciones:
    - Seleccione **Importar desde directorio** y, a continuación, vaya al directorio raíz que contiene los proyectos que desea añadir. Marque el cuadro de selección **Realizar recursividad en subdirectorios** para buscar en subdirectorios.
    - Seleccione **Importar desde el espacio de trabajo basado en Eclipse**. Seleccione el **Tipo de espacio de trabajo** y, a continuación, vaya al espacio de trabajo. Seleccione el directorio del espacio de trabajo y luego pulse **Aceptar**.
    - Seleccione **Importar desde un archivo de Microsoft Solution**. Examine el archivo, selecciónelo y luego pulse **Aceptar**.
  4. Realice una de estas acciones:
    - Pulse **Finalizar** para añadir los proyectos a la aplicación.
    - Pulse **Siguiente** para ver los resultados de la búsqueda y seleccionar los proyectos que se han de añadir. Luego pulse **Finalizar**.

**Importante:** Si está trabajando con un proyecto AppScan Source que tiene dependencias en un entorno de desarrollo, por ejemplo, un proyecto de IBM MobileFirst Platform, asegúrese de que crea el proyecto en el entorno de desarrollo antes de importarlo. Después de importar el proyecto, si modifica los archivos que contiene, asegúrese de que vuelve a crearlo en el entorno de desarrollo antes del escaneo en AppScan Source. Si no lo hace, AppScan Source omite las modificaciones que se realicen en los archivos.

## Adición de varios proyectos con arrastrar y soltar

### Procedimiento

1. En la estación de trabajo, localice los proyectos (.ppf, .vcproj, .dsp, .vbproj o .csproj) que desea añadir para escanear.

**Nota:** No es posible arrastrar y soltar archivos creados por ninguna de las herramientas de integración de compilación soportadas (como, por ejemplo, Ounce/Maven o Ounce/Ant).

2. Seleccione los proyectos, o realice una selección múltiple de los mismos, y arrástrelos a la vista Explorador.
3. Suelte la selección en una aplicación existente.

**Nota:** También puede soltar la selección en el nodo **Todas las aplicaciones** o bajo el mismo, aunque no se recomienda hacerlo. Resulta más aconsejable soltar varios proyectos en una aplicación existente, o individualmente, si se necesitan nuevas aplicaciones.

Puesto que los proyectos deben estar contenidos en una aplicación y al soltar proyectos en el nodo **Todas las aplicaciones** o bajo el mismo no se añade el proyecto a una explicación existente, el Asistente para aplicaciones nuevas le solicitará que cree una nueva aplicación para cada proyecto que esté añadiendo a la vista.

Para añadir varios proyectos a una aplicación nueva que aún no exista, cree primero la aplicación y luego arrastre y suelte los proyectos seleccionados en la misma.

**Importante:** Si está trabajando con un proyecto AppScan Source que tiene dependencias en un entorno de desarrollo, por ejemplo, un proyecto de IBM MobileFirst Platform, asegúrese de que crea el proyecto en el entorno de

desarrollo antes de importarlo. Después de importar el proyecto, si modifica los archivos que contiene, asegúrese de que vuelve a crearlo en el entorno de desarrollo antes del escaneo en AppScan Source. Si no lo hace, AppScan Source omite las modificaciones que se realicen en los archivos.

## Adición de un nuevo proyecto Arxan

El Asistente de configuración de proyecto le ayuda a crear manualmente un proyecto Arxan y a añadirlo a una aplicación.

### Acerca de esta tarea

Los pasos de este tema le indican cómo completar todas las páginas del Asistente de proyecto nuevo (o el Asistente para nueva aplicación, si está creando el proyecto en el mismo). Los valores del asistente se pueden modificar después de crear el proyecto en la vista Propiedades para un proyecto seleccionado.

### Procedimiento

1. En la vista Explorador, seleccione la aplicación a la que desea añadir el proyecto (si aún no ha añadido una aplicación, consulte “Configuración de aplicaciones” en la página 36).
2. Realice una de estas acciones para abrir el Asistente de proyecto nuevo:
  - a. Seleccione **Archivo > Añadir proyecto > Proyecto nuevo** en el menú principal del espacio de trabajo.
  - b. Pulse con el botón derecho en la aplicación seleccionada y elija **Añadir proyecto > Proyecto nuevo** en el menú de contexto.
3. En la página Seleccionar tipo de proyecto del asistente, seleccione **Arxan Android** o **Arxan iOS** como tipo de proyecto y pulse **Siguiente** para avanzar a la siguiente página del asistente.
4. En la página del asistente de orígenes de proyecto:
  - a. Identifique los orígenes de proyecto. Los orígenes de un proyecto constan de los directorios en los que se encuentran los archivos del proyecto y de cualquier archivo individuales adicionales que se ha de incluir en el proyecto.  
Asigne un nombre al proyecto y especifique el directorio de trabajo. El **Directorio de trabajo** es la ubicación en la que residirá el archivo de proyecto de AppScan Source (.ppf). También es la base para todas las vías de acceso relativas.
  - b. Pulse **Añadir raíz del origen** para especificar una raíz del código fuente y los directorios o archivos que desea incluir en el escaneo o excluir del mismo. Después de añadir la raíz del origen, puede excluir de la misma ciertos directorios o archivos. Para ello, seleccione el directorio o archivo (o realice una selección múltiple de estos elementos) en la raíz de origen, pulse con el botón derecho en la selección y elija **Excluir** en el menú. Si incluye o excluye archivos, el icono que hay a la izquierda del nombre del archivo cambia.
5. Pulse **Finalizar**.

## Adición de un nuevo proyecto ASP

El Asistente de configuración de proyecto le ayuda a crear manualmente un proyecto ASP y a añadirlo a una aplicación.

## Acerca de esta tarea

**Nota:** Este tipo de proyecto está soportado sólo en Windows.

Los pasos de este tema le indican cómo completar todas las páginas del Asistente de proyecto nuevo (o el Asistente para nueva aplicación, si está creando el proyecto en el mismo). Sin embargo, algunas de las páginas del asistente son opcionales (los valores necesarios se han completado cuando el botón **Finalizar** está activado). Los valores del asistente se pueden modificar después de crear el proyecto en la vista Propiedades para un proyecto seleccionado. Si completa el Asistente de proyecto nuevo sin completar las páginas opcionales, puede cambiar los valores de estas páginas más adelante en la vista Propiedades.

**Nota:** Para PHP, VB6 y Classic ASP, sólo se da soporte a conjuntos de caracteres ISO-8859-1 (Europeo occidental), UTF-8 y UTF-16.

## Procedimiento

1. En la vista Explorador, seleccione la aplicación a la que desea añadir el proyecto (si aún no ha añadido una aplicación, consulte “Configuración de aplicaciones” en la página 36).
2. Realice una de estas acciones para abrir el Asistente de proyecto nuevo:
  - a. Seleccione **Archivo > Añadir proyecto > Proyecto nuevo** en el menú principal del espacio de trabajo.
  - b. Pulse con el botón derecho en la aplicación seleccionada y elija **Añadir proyecto > Proyecto nuevo** en el menú de contexto.
3. En la página Seleccionar tipo de proyecto del asistente, seleccione **ASP** como tipo de proyecto y pulse **Siguiente** para avanzar a la siguiente página del asistente.
4. En la página del asistente de orígenes de proyecto:
  - a. Identifique los orígenes de proyecto. Los orígenes de un proyecto constan de los directorios en los que se encuentran los archivos del proyecto y de cualquier archivo individuales adicionales que se ha de incluir en el proyecto.  
Asigne un nombre al proyecto y especifique el directorio de trabajo. El **Directorio de trabajo** es la ubicación en la que residirá el archivo de proyecto de AppScan Source (.ppf). También es la base para todas las vías de acceso relativas.
  - b. Pulse **Añadir raíz del origen** para especificar una raíz del código fuente y los directorios o archivos que desea incluir en el escaneo o excluir del mismo. Después de añadir la raíz del origen, puede excluir de la misma ciertos directorios o archivos. Para ello, seleccione el directorio o archivo (o realice una selección múltiple de estos elementos) en la raíz de origen, pulse con el botón derecho en la selección y elija **Excluir** en el menú. Si incluye o excluye archivos, el icono que hay a la izquierda del nombre del archivo cambia.
5. Pulse **Siguiente** para avanzar a la siguiente página del asistente.
6. En la página Configuración de proyecto ASP:
  - a. Configure el proyecto ASP identificando la raíz de contenido ASP y el lenguaje predeterminado:  
**Raíz de contenido ASP:** directorio correspondiente a la URL principal de la web o del dominio  
**Lenguaje predeterminado:** VB Script (valor predeterminado) o JavaScript

- b. Añada, suprima o mueva las Bibliotecas de tipos (dll, exe, ocx o tlb) de las que depende el proyecto ASP para la compilación.
7. Pulse **Finalizar**.

## Adición de un nuevo proyecto C/C++

### Acerca de esta tarea

Cuando añada un nuevo proyecto C/C++ a la aplicación, especifica una colección de archivos de origen que se deben escanear:

- vía de acceso include
- definiciones de preprocesador
- opciones

Los pasos de este tema le indican cómo completar todas las páginas del Asistente de proyecto nuevo (o el Asistente para nueva aplicación, si está creando el proyecto en el mismo). Sin embargo, algunas de las páginas del asistente son opcionales (los valores necesarios se han completado cuando el botón **Finalizar** está activado). Los valores del asistente se pueden modificar después de crear el proyecto en la vista Propiedades para un proyecto seleccionado. Si completa el Asistente de proyecto nuevo sin completar las páginas opcionales, puede cambiar los valores de estas páginas más adelante en la vista Propiedades.

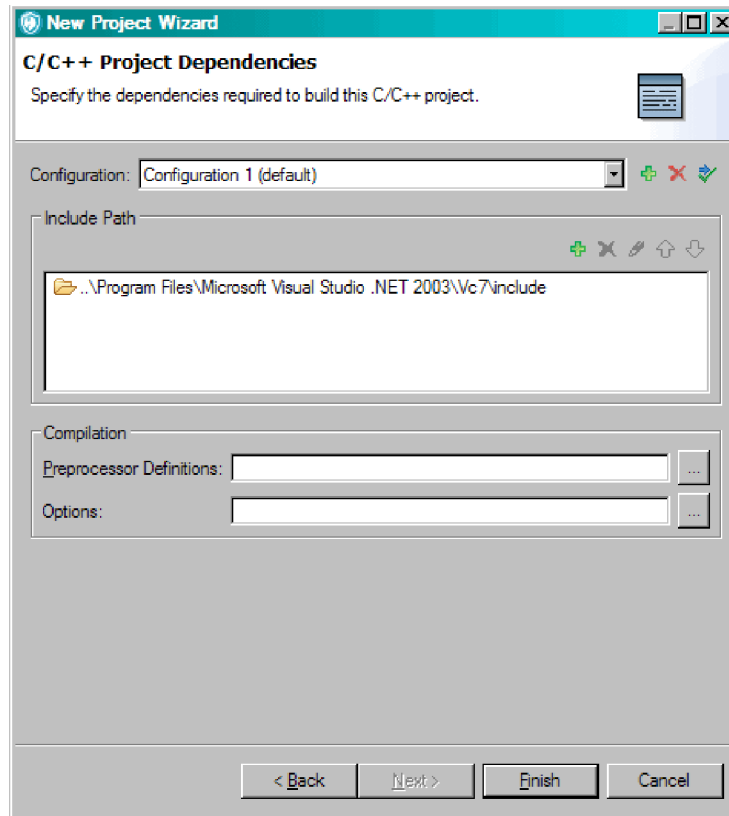
**Importante:** Para poder escanear un proyecto C++, el proyecto se debe compilar y enlazar sin errores.

### Procedimiento

1. En la vista Explorador, seleccione la aplicación a la que desea añadir el proyecto (si aún no ha añadido una aplicación, consulte “Configuración de aplicaciones” en la página 36).
2. Realice una de estas acciones para abrir el Asistente de proyecto nuevo:
  - a. Seleccione **Archivo > Añadir proyecto > Proyecto nuevo** en el menú principal del espacio de trabajo.
  - b. Pulse con el botón derecho en la aplicación seleccionada y elija **Añadir proyecto > Proyecto nuevo** en el menú de contexto.
3. En la página Seleccionar tipo de proyecto del asistente, seleccione **C/C++** como tipo de proyecto y pulse **Siguiente** para pasar a la siguiente página del asistente.
4. En la página del asistente de orígenes de proyecto:
  - a. Identifique los orígenes de proyecto. Los orígenes de un proyecto constan de los directorios en los que se encuentran los archivos del proyecto y de cualquier archivo individuales adicionales que se ha de incluir en el proyecto.  
Asigne un nombre al proyecto y especifique el directorio de trabajo. El **Directorio de trabajo** es la ubicación en la que residirá el archivo de proyecto de AppScan Source (.ppf). También es la base para todas las vías de acceso relativas.
  - b. Pulse **Añadir raíz del origen** para especificar una raíz del código fuente y los directorios o archivos que desea incluir en el escaneo o excluir del mismo. Después de añadir la raíz del origen, puede excluir de la misma ciertos directorios o archivos. Para ello, seleccione el directorio o archivo (o realice una selección múltiple de estos elementos) en la raíz de origen, pulse

con el botón derecho en la selección y elija **Excluir** en el menú. Si incluye o excluye archivos, el icono que hay a la izquierda del nombre del archivo cambia.

5. Pulse **Siguiente** para avanzar a la siguiente página del asistente.
6. En la página Dependencias de proyecto C/C++, añada las dependencias del proyecto, especificando la configuración del proyecto y la vía de acceso include.



- **Configuración:** lista de todas las configuraciones disponibles para el proyecto. Añada nuevas configuraciones o suprima configuraciones existentes. Defina todos los valores restantes para cada configuración. Puede definir varias configuraciones para un proyecto C/C++, como por ejemplo Depurar y Release. Configuración 1 es el nombre predeterminado de la configuración del proyecto.
- **Vías de acceso de inclusión:** Utilice esta sección para añadir los nombres de vía de acceso completos a los directorios que contienen los archivos `#include` necesarios para el proyecto.
- **Definiciones del preprocesador:** Utilice este campo para añadir símbolos de preproceso definidos para el proyecto. Las definiciones de preprocesador son específicas del código C/C++. Al especificar definiciones de preprocesador, no incluya la opción `-D` del compilador (por ejemplo, especifique `a=definition1` en lugar de `-Da=definition1`). Al especificar varios destinos, utilice una lista delimitada por puntos y comas.
- **Opciones:** parámetros necesarios del compilador adicionales para la configuración del proyecto.

7. Pulse **Finalizar**.



## Adición de un nuevo proyecto COBOL

El Asistente de configuración de proyecto le ayuda a crear manualmente un proyecto COBOL y a añadirlo a una aplicación.

### Acerca de esta tarea

Los pasos de este tema le indican cómo completar todas las páginas del Asistente de proyecto nuevo (o el Asistente para nueva aplicación, si está creando el proyecto en el mismo). Los valores del asistente se pueden modificar después de crear el proyecto en la vista Propiedades para un proyecto seleccionado.

### Procedimiento

1. En la vista Explorador, seleccione la aplicación a la que desea añadir el proyecto (si aún no ha añadido una aplicación, consulte “Configuración de aplicaciones” en la página 36).
2. Realice una de estas acciones para abrir el Asistente de proyecto nuevo:
  - a. Seleccione **Archivo > Añadir proyecto > Proyecto nuevo** en el menú principal del espacio de trabajo.
  - b. Pulse con el botón derecho en la aplicación seleccionada y elija **Añadir proyecto > Proyecto nuevo** en el menú de contexto.
3. En la página Seleccionar tipo de proyecto del asistente, seleccione **COBOL** como tipo de proyecto y pulse **Siguiente** para pasar a la siguiente página del asistente.
4. En la página del asistente de orígenes de proyecto:
  - a. Identifique los orígenes de proyecto. Los orígenes de un proyecto constan de los directorios en los que se encuentran los archivos del proyecto y de cualquier archivo individuales adicionales que se ha de incluir en el proyecto.  
Asigne un nombre al proyecto y especifique el directorio de trabajo. El **Directorio de trabajo** es la ubicación en la que residirá el archivo de proyecto de AppScan Source (.ppf). También es la base para todas las vías de acceso relativas.
  - b. Pulse **Añadir raíz del origen** para especificar una raíz del código fuente y los directorios o archivos que desea incluir en el escaneo o excluir del mismo. Después de añadir la raíz del origen, puede excluir de la misma ciertos directorios o archivos. Para ello, seleccione el directorio o archivo (o realice una selección múltiple de estos elementos) en la raíz de origen, pulse con el botón derecho en la selección y elija **Excluir** en el menú. Si incluye o excluye archivos, el icono que hay a la izquierda del nombre del archivo cambia.
5. Pulse **Finalizar**.

## Adición de un nuevo proyecto ColdFusion

El Asistente de configuración de proyecto le ayuda a crear manualmente un proyecto ColdFusion y a añadirlo a una aplicación.

### Acerca de esta tarea

Los pasos de este tema le indican cómo completar todas las páginas del Asistente de proyecto nuevo (o el Asistente para nueva aplicación, si está creando el proyecto en el mismo). Los valores del asistente se pueden modificar después de crear el proyecto en la vista Propiedades para un proyecto seleccionado.

## Procedimiento

1. En la vista Explorador, seleccione la aplicación a la que desea añadir el proyecto (si aún no ha añadido una aplicación, consulte “Configuración de aplicaciones” en la página 36).
2. Realice una de estas acciones para abrir el Asistente de proyecto nuevo:
  - a. Seleccione **Archivo > Añadir proyecto > Proyecto nuevo** en el menú principal del espacio de trabajo.
  - b. Pulse con el botón derecho en la aplicación seleccionada y elija **Añadir proyecto > Proyecto nuevo** en el menú de contexto.
3. En la página Seleccionar tipo de proyecto del asistente, seleccione **ColdFusion** como tipo de proyecto y pulse **Siguiente** para pasar a la siguiente página del asistente.
4. En la página del asistente de orígenes de proyecto:
  - a. Identifique los orígenes de proyecto. Los orígenes de un proyecto constan de los directorios en los que se encuentran los archivos del proyecto y de cualquier archivo individuales adicionales que se ha de incluir en el proyecto.  
Asigne un nombre al proyecto y especifique el directorio de trabajo. El **Directorio de trabajo** es la ubicación en la que residirá el archivo de proyecto de AppScan Source (.ppf). También es la base para todas las vías de acceso relativas.
  - b. Pulse **Añadir raíz del origen** para especificar una raíz del código fuente y los directorios o archivos que desea incluir en el escaneo o excluir del mismo. Después de añadir la raíz del origen, puede excluir de la misma ciertos directorios o archivos. Para ello, seleccione el directorio o archivo (o realice una selección múltiple de estos elementos) en la raíz de origen, pulse con el botón derecho en la selección y elija **Excluir** en el menú. Si incluye o excluye archivos, el icono que hay a la izquierda del nombre del archivo cambia.
5. Pulse **Finalizar**.

## Adición de un nuevo proyecto Java o JavaServer Page (JSP)

Cuando añade un nuevo proyecto Java a la aplicación, especifica el nombre del proyecto, va al directorio de trabajo y especifica las raíces de origen y las dependencias del proyecto.

### Acerca de esta tarea

Los pasos de este tema le indican cómo completar todas las páginas del Asistente de proyecto nuevo (o el Asistente para nueva aplicación, si está creando el proyecto en el mismo). Sin embargo, algunas de las páginas del asistente son opcionales (los valores necesarios se han completado cuando el botón **Finalizar** está activado). Los valores del asistente se pueden modificar después de crear el proyecto en la vista Propiedades para un proyecto seleccionado. Si completa el Asistente de proyecto nuevo sin completar las páginas opcionales, puede cambiar los valores de estas páginas más adelante en la vista Propiedades.

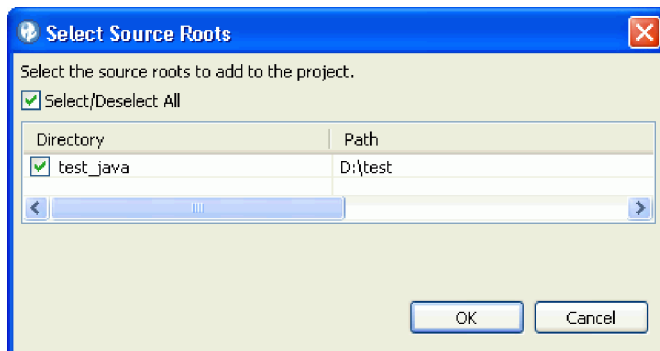
## Procedimiento

1. En la vista Explorador, seleccione la aplicación a la que desea añadir el proyecto (si aún no ha añadido una aplicación, consulte “Configuración de aplicaciones” en la página 36).
2. Realice una de estas acciones para abrir el Asistente de proyecto nuevo:

- a. Seleccione **Archivo > Añadir proyecto > Proyecto nuevo** en el menú principal del espacio de trabajo.
- b. Pulse con el botón derecho en la aplicación seleccionada y elija **Añadir proyecto > Proyecto nuevo** en el menú de contexto.
3. En la página Seleccionar tipo de proyecto del asistente, seleccione **Java/JSP** como tipo de proyecto y pulse **Siguiente** para avanzar a la siguiente página del asistente.
4. En la página del asistente de orígenes de proyecto:
  - a. Identifique los orígenes del proyecto, que constan de los directorios en los que se encuentran los archivos del proyecto y cualquier archivo individual adicional que desee incluir en el proyecto.  
 Asigne un nombre al proyecto y especifique el directorio de trabajo. El **Directorio de trabajo** es la ubicación del archivo de proyecto de AppScan Source (.ppf) y la base para todas las vías de acceso relativas.
  - b. Añada las raíces de origen manualmente o deje que AppScan Source for Analysis busque automáticamente todas las raíces de origen válidas.

#### Importante:

- Para analizar archivos de clase Java, deben estar compilados con javac utilizando la opción -g. El análisis de AppScan Source se basa en la información de depuración generada por esta opción.
- Si el proyecto contiene archivos de origen de Java que contienen caracteres nacionales y está trabajando en un entorno local que no es el nativo (por ejemplo, UTF-8), el escaneo fallará con errores y/o con avisos en la consola.
- Para buscar las raíces de origen automáticamente:
  - 1) Pulse **Buscar raíces del origen** y vaya al directorio raíz del código fuente.
  - 2) En la lista de raíces de origen encontradas, seleccione las raíces de origen que desea añadir al proyecto.

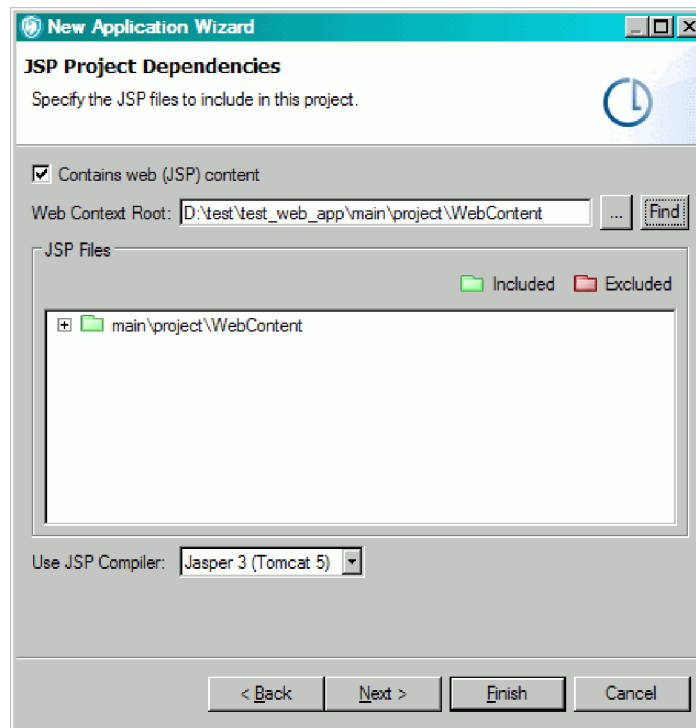


- 3) Pulse en **Aceptar**. Los orígenes que se incluirán en el escaneo aparecen en el recuadro de diálogo **Orígenes de proyecto**.
- Para buscar manualmente las raíces de origen:
  - 1) Pulse **Añadir raíz del origen**.
  - 2) Seleccione el directorio raíz o archivo del código fuente.
  - 3) Pulse en **Aceptar**. Después de añadir la raíz del origen, puede excluir de la misma ciertos directorios o archivos. Para ello, seleccione el directorio o archivo (o realice una selección múltiple de estos elementos), pulse con el botón derecho en la selección y elija **Excluir**.

en el menú. Si incluye o excluye archivos, el icono que hay a la izquierda del nombre del archivo cambia.

Pulse **Finalizar** para añadir el proyecto sin establecer dependencias del proyecto, o bien pulse **Siguiente** para identificar dependencias del proyecto.

5. En la página Dependencias del proyecto JSP:
  - a. Identifique las dependencias del proyecto JavaServer Page (JSP): para proyectos Java que contienen JavaServer Pages, identifique las dependencias del proyecto JSP. Marque el cuadro de selección **Contiene contenido (JSP) web** si el proyecto es una aplicación web que contiene JavaServer Pages.



- b. Seleccione manualmente la **Raíz de contexto web** o pulse en **Buscar** para localizarla. La **Raíz de contexto web** es un archivo WAR o un directorio que contiene el directorio WEB-INF. La raíz de contexto web debe ser la raíz de una aplicación web válida.
  - c. Seleccione el **Compilador JSP** correspondiente al proyecto. Tomcat 7, listo para utilizar, es el valor de compilador JSP predeterminado (el compilador JSP predeterminado se puede modificar en la página de preferencias de Java y JSP). Para conocer los compiladores a los que AppScan Source da soporte, consulte <http://www.ibm.com/support/docview.wss?uid=swg27027486>.

La instalación de AppScan Source incluye Apache Tomcat Versiones 7 y 8. Si las páginas de preferencias de **Tomcat 7** y **Tomcat 8** no están configuradas, AppScan Source compilará los archivos JSP mediante el compilador Tomcat JSP proporcionado que actualmente está marcado como predeterminado. Si desea utilizar un compilador Tomcat soportado externo, utilice la página de preferencias de Tomcat para apuntar a la instalación local de Tomcat.

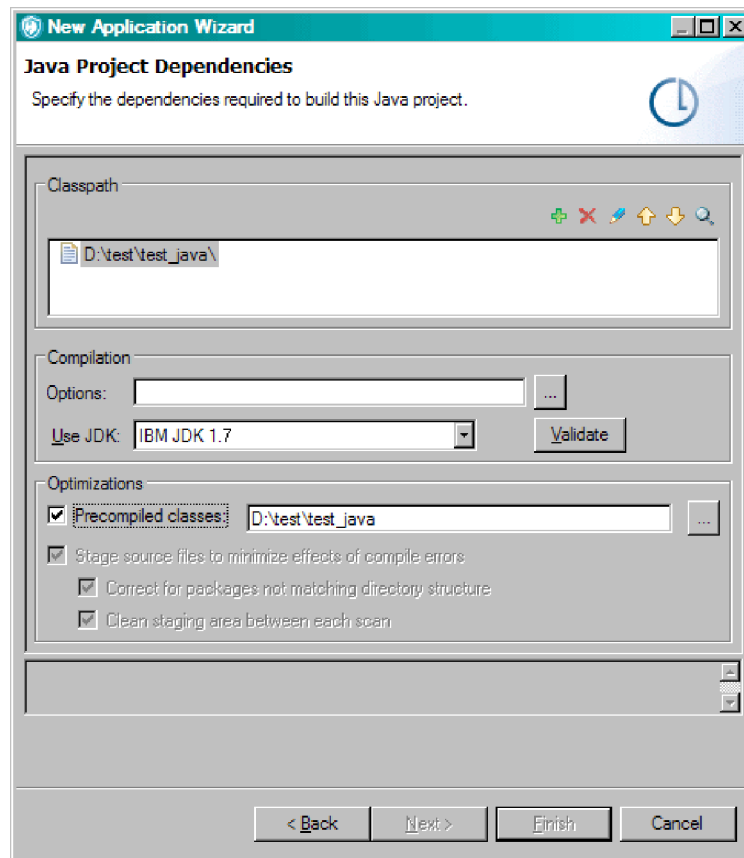
Si utiliza un servidor de aplicaciones Oracle WebLogic Server o WebSphere Application Server, debe configurar la página de preferencias correspondiente para que apunte a la instalación local del servidor de aplicaciones a fin de que se pueda utilizar para la compilación de JSP durante el análisis. Si aún no ha finalizado esta configuración, se le solicitará mediante un mensaje el que lo haga cuando se seleccione el

compilador JSP. Si pulsa **Sí** en el mensaje, se le llevará a la página de preferencias adecuada. Si pulsa **No**, un enlace de aviso aparecerá junto a la selección del compilador JSP (siguiendo dicho enlace se abrirá la página de preferencias).

Pulse **Finalizar** para añadir el proyecto con dependencias de proyecto JSP, o bien pulse **Siguiente** para identificar las dependencias del proyecto Java.

6. En la página Dependencias del proyecto Java, identifique las dependencias necesarias para crear este proyecto Java:
  - a. Añada los archivos JAR manualmente o pulse **Buscar** para que AppScan Source for Analysis busque los directorios que contienen los archivos JAR y de clase dependientes.

La lista de **vías de acceso de clases** muestra la vía de acceso relativas del proyecto. La vía de acceso de clase debe especificar los archivos JAR necesarios y los directorios que contienen los archivos de clase que necesita el proyecto.



- **Añadir, Eliminar, Mover arriba y Mover abajo:** añada o elimine archivos de la vía de acceso de clase, o súbalos o bájelos por orden.
- **Buscar:** busca las entradas JAR y de vía de acceso de clase basadas en los archivos de origen del proyecto.

**Importante:** Si el proyecto Java contiene JavaServer Pages, también debe añadir las dependencias del proyecto JSP.

- Para buscar manualmente las dependencias del proyecto:
  - 1) Pulse **Añadir** en la barra de herramientas de la sección Vía de acceso de clase y seleccione los directorios JAR y de archivos de clase necesarios para compilar el proyecto Java.

- 2) Pulse en **Aceptar**. Los archivos JAR y los directorios aparecen en la vía de acceso de clase. Cambie el orden si hace falta.
- Para buscar dependencias automáticamente:
    - 1) Pulse **Buscar** en la barra de herramientas de la sección Vía de acceso de clase.
    - 2) Especifique los directorios en los que se han de buscar los archivos de clases y JAR necesarios para compilar el proyecto Java.
    - 3) Seleccione el cuadro de selección **Mirar dentro de archivos JAR y origen** si desea que AppScan Source for Analysis busque las dependencias del proyecto necesarias en función de los orígenes y utilizando la vía de acceso de búsqueda especificada.
    - 4) Pulse **Siguiente** para buscar las dependencias del proyecto e identificar los conflictos.
  - Para resolver conflictos:
    - 1) Si existen conflictos, en el cuadro de diálogo Resolver conflictos, seleccione la entrada que desea resolver y pulse **Resolver** (o pulse **Siguiente** para resolver los conflictos automáticamente). Se produce un conflicto cuando AppScan Source for Analysis encuentra más de un archivo JAR o de clase en un directorio que satisface la dependencia.  
Aparece un icono rojo a la izquierda de los conflictos no resueltos. Una vez resuelto el conflicto, el icono rojo se pone verde y el elemento aparece como **Resuelto**. También puede **Eliminar** un conflicto.
    - 2) Después de solucionar o de eliminar un conflicto, es posible que desee verificar, reordenar o eliminar las entradas de la vía de acceso de clase. Tenga en cuenta la lista de importaciones que no se han encontrado. Las importaciones no resueltas dan lugar a errores de compilación cuando AppScan Source for Analysis realiza escaneos.
- b. **Opciones:** especificar cualquier parámetro adicional del compilador necesario para la configuración del proyecto.
- Las opciones de compilación son las opciones que se pasan al compilador, de modo que pueda compilar archivos de origen. Por ejemplo, `-source 1.5` especifica el nivel de origen del proyecto.
- c. **Utilizar JDK:** especifique el JDK (Java Development Kit) que se debe utilizar para escanear este código. De forma predeterminada, se utilizará **IBM JDK 1.8**. AppScan Source también proporciona **IBM JDK 1.7** para su selección. Para definir los JDK adicionales, o para definir un JDK predeterminado distinto, utilice las **Preferencias de Java y JSP**.
- Nota:** El compilador predeterminado, listo para utilizar, para los proyectos JSP es Tomcat 7, y necesita Java Versión 1.6 o superior. Si se mantiene **Tomcat 7** como predeterminado, utilizar un JDK anterior provocará errores de compilación durante los escaneos.
- d. La acción **Validar** asegura que las dependencias del proyecto estén correctamente configuradas. Comprueba los proyectos Java para ver si hay conflictos de configuración entre los orígenes y la vía de acceso de clase y comprueba si existen errores de compilación. Existe un conflicto si una clase de la vía de acceso de clase está duplicada en la raíz del origen.
- Si existe un conflicto, el área de texto de validación muestra el archivo JAR o la ubicación en la que está definida la clase en la vía de acceso de clase y si

la duplicación se encuentra en los orígenes. Elimine el conflicto de la vía de acceso de clase y vuelva a ejecutar la comprobación.

Después de comprobar si existen conflictos, **Validar** determina si el proyecto se compila y notifica cualquier error de compilación.

- e. **Clases precompiladas:** este campo le permite utilizar archivos de clase precompilados Java o JSP, en lugar de realizar la compilación durante un escaneo.
  - f. **Organizar archivos de origen para minimizar los efectos de errores de compilación:** borre el cuadro de selección si el código fuente se compila correctamente y está adecuadamente organizado en directorios que coinciden con los paquetes.
  - g. **Corregir los paquetes que no coincidan con la estructura de directorios:** seleccione esta opción si los paquetes no coinciden con la estructura de directorios.
  - h. **Limpiar el área de transferencia entre cada escaneo:** opción de optimización.
7. Pulse **Finalizar**.

## Resultados

**Consejo:** Si está escaneando Java y faltan dependencias en el proyecto de Java, AppScan Source creará rastreos sintetizando las partes que las dependencias hayan proporcionado. Esta síntesis puede que no refleje de forma precisa la información en archivos .jar. Para limitar la síntesis y mejorar la precisión de los resultados, puede especificar las dependencias que faltan, como por ejemplo:

1. Tras escanear, abra <data\_dir>\logs\scanner\_exceptions.log (donde <data\_dir> es la ubicación de los datos de programa AppScan Source, como se describe en “Instalación y ubicaciones de archivo de datos de usuario” en la página 335) para ver si a AppScan Source le faltan dependencias de las que se ha informado.
2. Modifique las propiedades de proyecto para que incluyan las dependencias. Para ello, siga las instrucciones de “Modificación de las propiedades del proyecto y de la aplicación” en la página 83 y, a continuación, especifique y guarde las dependencias en el separador **Dependencias del proyecto JSP** o **Dependencias del proyecto**.
3. Vuelva a escanear el proyecto.

**Nota:** De forma predeterminada, AppScan Source escanea archivos Java y código de bytes de Java con dependencias o errores de compilación perdidos. Estos valores se pueden modificar como se indica a continuación:

1. Abra <data\_dir>\config\scan.ozsettings en un editor de textos.
2. Para cambiar el valor de error de compilación, ubique compile\_java\_sources\_with\_errors en el archivo. Este valor es similar a:

```
<Setting
  name="compile_java_sources_with_errors"
  value="true"
  default_value="true"
  type="bool"
  hidden="true"
  display_name="compile_java_sources_with_errors"
  description="Intento de escanear código java con errores de compilación".
/>
```

- Para modificar el valor de dependencia que falta, ubique `scan_java_bytecode_without_dependencies` en el archivo. Este valor es similar a:

```
<Setting
  name="scan_java_bytecode_without_dependencies"
  value="true"
  default_value="true"
  type="bool"
  hidden="true"
  display_name="scan_java_bytecode_without_dependencies"
  description="Escanea el código de bytes de Java incluso cuando algunas de
    las dependencias faltan mediante la sintetización artificial
    de los símbolos no resueltos".
/>
```

- En el valor, modifique el atributo `value`. Si el atributo se establece en `true`, este valor estará activo. Si el valor de error de compilación está establecido en `false`, AppScan Source omitirá el código Java con errores de compilación durante los escaneos. Si el valor de dependencia que falta está establecido en `false`, AppScan Source no escaneará el código de bytes Java si faltan dependencias.
- Guarde el archivo una vez que haya modificado este valor e inicie o reinicie AppScan Source.

## Adición de contenido a un proyecto JSP

Los proyectos JavaServer Page (JSP) incluyen aplicaciones web basadas en JavaServer Pages.

### Acerca de esta tarea

Para escanear correctamente proyectos JSP, JavaServer Pages debe estar en una estructura válida de la aplicación web. En esta sección se describe la estructura de archivos bajo la raíz del contexto web necesaria para realizar escaneos correctamente. Debe estar familiarizado con la estructura de la aplicación web antes de configurar proyectos JSP.

Una aplicación web desplegada en un servidor de aplicaciones web, como por ejemplo Tomcat, necesita una estructura de directorios estándar. La aplicación desplegada puede ser un conjunto de archivos organizados en una estructura de directorios o un archivo WAR. En el caso de un archivo WAR, la estructura de directorios está contenida en el archivo ZIP y la raíz de contexto web es la raíz de la estructura de directorios.

Bajo una raíz de contexto web, se encuentran los siguientes directorios estándares:

*Tabla 6. Directorios de la raíz de contexto web*

|                     |                                                              |
|---------------------|--------------------------------------------------------------|
| <web-context-root>\ |                                                              |
| WEB-INF\            |                                                              |
| classes\            | Archivos de clase Java organizados en directorios (paquetes) |
| lib\                | Archivos JAR añadidos a la vía de acceso de clase            |
| web.xml             | web.xml describe los recursos disponibles para la aplicación |



Otros directorios contienen los archivos necesarios que puede haber. Por ejemplo, con frecuencia verá un directorio para el contenido (archivos JSP y HTML) y para las bibliotecas de códigos (tag):

*Tabla 7. Otros directorios*

|                     |                                                                      |
|---------------------|----------------------------------------------------------------------|
| <web-context-root>\ |                                                                      |
| jsp\                | Contiene JavaServer Pages de la aplicación                           |
| WEB-INF\            |                                                                      |
| tld\                | Contiene las bibliotecas de códigos que se utilizan en la aplicación |

Además de estos directorios estándares de aplicaciones web, un servidor de aplicaciones web puede tener directorios especiales en los que espera encontrar los archivos de clase y archivos JAR compartidos por todas las aplicaciones web desplegadas. Por ejemplo, Tomcat 7 ubica estos archivos JAR en los directorios `common\lib` o `common\endorsed`. La ubicación de estos directorios no estándares es específica de cada servidor de aplicaciones.

**Importante:** Antes de escanear JavaServer Pages, confirme que todos los archivos necesarios existen en la raíz de contexto web. AppScan Source for Analysis solo escanea JavaServer Pages en la raíz de contexto web.

## Procedimiento

1. Copie los archivos, si es necesario, en la ubicación adecuada bajo la raíz de contexto web.
2. Especifique la raíz de contexto web como el directorio o como un archivo WAR que contenga todas las JavaServer Pages.
3. Asegúrese de que la vía de acceso de clase incluya los directorios de los archivos JAR o de los archivos de clase.
4. Configure las propiedades del proyecto.

## Resultados

AppScan Source for Analysis añade el directorio `WEB-INF\classes` y todos los archivos JAR de `WEB-INF\lib` a la vía de acceso de clase, solo para JSP. Puede añadir elementos que no estén incluidos en la vía de acceso `Web-INF` pero que sean necesarios para compilar JSP. Estos archivos JAR se parecen a `weblogic.jar` o a un archivo JAR de otro proveedor colocado en el directorio común para un servidor de aplicaciones.

Los orígenes JSP son JavaServer Pages bajo la raíz de contexto web que desea escanear. Los archivos de origen son relativos a la raíz de contexto web. Está limitado al conjunto de archivos dentro de la raíz de contexto web cuando especifique los orígenes de JSP.

Los orígenes de un proyecto JSP son los directorios en los que se encuentran los archivos del proyecto y los archivos individuales adicionales que desea incluir en el proyecto.

- Especifique el subconjunto de JavaServer Pages en la raíz de contexto web. Si no lo hace, se escanearán todos los archivos.
- Si JavaServer Pages depende del código Java, debe especificar estos orígenes.
- Los archivos JSP incluyen archivos `jsp` y `jspx`.

## Adición de un nuevo proyecto de JavaScript

El asistente de configuración de proyectos ayuda a crear de forma manual un proyecto de JavaScript y a añadirlo a una aplicación.

### Acerca de esta tarea

Los pasos de este tema le indican cómo completar todas las páginas del Asistente de proyecto nuevo (o el Asistente para nueva aplicación, si está creando el proyecto en el mismo). Los valores del asistente se pueden modificar después de crear el proyecto en la vista Propiedades para un proyecto seleccionado.

### Procedimiento

1. En la vista Explorador, seleccione la aplicación a la que desea añadir el proyecto (si aún no ha añadido una aplicación, consulte “Configuración de aplicaciones” en la página 36).
2. Realice una de estas acciones para abrir el Asistente de proyecto nuevo:
  - a. Seleccione **Archivo > Añadir proyecto > Proyecto nuevo** en el menú principal del espacio de trabajo.
  - b. Pulse con el botón derecho en la aplicación seleccionada y elija **Añadir proyecto > Proyecto nuevo** en el menú de contexto.
3. En la página Seleccionar tipo de proyecto del asistente, seleccione **JavaScript** como tipo de proyecto y pulse **Siguiente** para pasar a la siguiente página del asistente.
4. En la página del asistente de orígenes de proyecto:
  - a. Identifique los orígenes de proyecto. Los orígenes de un proyecto constan de los directorios en los que se encuentran los archivos del proyecto y de cualquier archivo individuales adicionales que se ha de incluir en el proyecto.  
Asigne un nombre al proyecto y especifique el directorio de trabajo. El **Directorio de trabajo** es la ubicación en la que residirá el archivo de proyecto de AppScan Source (.ppf). También es la base para todas las vías de acceso relativas.
  - b. Pulse **Añadir raíz del origen** para especificar una raíz del código fuente y los directorios o archivos que desea incluir en el escaneo o excluir del mismo. Después de añadir la raíz del origen, puede excluir de la misma ciertos directorios o archivos. Para ello, seleccione el directorio o archivo (o realice una selección múltiple de estos elementos) en la raíz de origen, pulse con el botón derecho en la selección y elija **Excluir** en el menú. Si incluye o excluye archivos, el icono que hay a la izquierda del nombre del archivo cambia.
5. Pulse **Finalizar**.

## Adición de un nuevo proyecto .NET Assembly

El Asistente de proyecto nuevo le ayuda a crear un proyecto .NET Assembly. Un proyecto .NET Assembly se puede utilizar para escanear archivos compilados de .NET Assembly, cuando los archivos de origen no estén disponibles o no se puedan crear. Los proyectos .NET Assembly consisten en un directorio de trabajo y una lista de orígenes, que pueden ser directorios o archivos de ensamblado individuales.

## Acerca de esta tarea

**Nota:** Este tipo de proyecto está soportado sólo en Windows.

Los pasos de este tema le indican cómo completar todas las páginas del Asistente de proyecto nuevo (o el Asistente para nueva aplicación, si está creando el proyecto en el mismo). Los valores del asistente se pueden modificar después de crear el proyecto en la vista Propiedades para un proyecto seleccionado.

## Procedimiento

1. En la vista Explorador, seleccione la aplicación a la que desea añadir el proyecto (si aún no ha añadido una aplicación, consulte “Configuración de aplicaciones” en la página 36).
2. Realice una de estas acciones para abrir el Asistente de proyecto nuevo:
  - a. Seleccione **Archivo > Añadir proyecto > Proyecto nuevo** en el menú principal del espacio de trabajo.
  - b. Pulse con el botón derecho en la aplicación seleccionada y elija **Añadir proyecto > Proyecto nuevo** en el menú de contexto.
3. En la página Seleccionar tipo de proyecto del asistente, seleccione **T-SQL** como tipo de proyecto y pulse **Siguiente** para avanzar a la siguiente página del asistente.
4. En la página del asistente de orígenes de proyecto:
  - a. Identifique los orígenes de proyecto. Los orígenes de un proyecto constan de los directorios en los que se encuentran los archivos del proyecto y de cualquier archivo individuales adicionales que se ha de incluir en el proyecto.  
Asigne un nombre al proyecto y especifique el directorio de trabajo. El **Directorio de trabajo** es la ubicación en la que residirá el archivo de proyecto de AppScan Source (.ppf). También es la base para todas las vías de acceso relativas.
  - b. Pulse **Añadir raíz del origen** para especificar una raíz del código fuente y los directorios o archivos que desea incluir en el escaneo o excluir del mismo. Después de añadir la raíz del origen, puede excluir de la misma ciertos directorios o archivos. Para ello, seleccione el directorio o archivo (o realice una selección múltiple de estos elementos) en la raíz de origen, pulse con el botón derecho en la selección y elija **Excluir** en el menú. Si incluye o excluye archivos, el icono que hay a la izquierda del nombre del archivo cambia.
5. Pulse **Finalizar**.

## Adición de un nuevo proyecto basado en patrón

### Acerca de esta tarea

El Asistente de nuevo proyecto le ayuda a crear manualmente un proyecto basado en patrón y añadirlo a una aplicación. Los proyectos basados en patrón incluyen una recopilación de cualquier archivo independiente de idioma para el análisis basado en patrón y para el escaneo.

Por ejemplo, es posible que desee agrupar lógicamente los archivos .xml y .config y buscarlos para determinadas expresiones basadas en patrón. AppScan Source for Analysis escanea los archivos y busca las expresiones (consulte la sección “Personalización con reglas basadas en patrón” en la página 247 para obtener información detallada).

Los pasos de este tema le indican cómo completar todas las páginas del Asistente de proyecto nuevo (o el Asistente para nueva aplicación, si está creando el proyecto en el mismo). Los valores del asistente se pueden modificar después de crear el proyecto en la vista Propiedades para un proyecto seleccionado.

## Procedimiento

1. En la vista Explorador, seleccione la aplicación a la que desea añadir el proyecto (si aún no ha añadido una aplicación, consulte “Configuración de aplicaciones” en la página 36).
2. Realice una de estas acciones para abrir el Asistente de proyecto nuevo:
  - a. Seleccione **Archivo > Añadir proyecto > Proyecto nuevo** en el menú principal del espacio de trabajo.
  - b. Pulse con el botón derecho en la aplicación seleccionada y elija **Añadir proyecto > Proyecto nuevo** en el menú de contexto.
3. En la página Seleccionar tipo de proyecto del asistente, seleccione **Basado en patrón** como tipo de proyecto y pulse **Siguiente** para pasar a la siguiente página del asistente.
4. En la página del asistente de orígenes de proyecto:
  - a. Identifique los orígenes de proyecto. Los orígenes de un proyecto constan de los directorios en los que se encuentran los archivos del proyecto y de cualquier archivo individuales adicionales que se ha de incluir en el proyecto.  
Asigne un nombre al proyecto y especifique el directorio de trabajo. El **Directorio de trabajo** es la ubicación en la que residirá el archivo de proyecto de AppScan Source (.ppf). También es la base para todas las vías de acceso relativas.
  - b. Pulse **Añadir raíz del origen** para especificar una raíz del código fuente y los directorios o archivos que desea incluir en el escaneo o excluir del mismo. Después de añadir la raíz del origen, puede excluir de la misma ciertos directorios o archivos. Para ello, seleccione el directorio o archivo (o realice una selección múltiple de estos elementos) en la raíz de origen, pulse con el botón derecho en la selección y elija **Excluir** en el menú. Si incluye o excluye archivos, el icono que hay a la izquierda del nombre del archivo cambia.
5. Pulse **Finalizar**.

## Adición de un nuevo proyecto Perl

El Asistente de nuevo proyecto le ayuda a crear manualmente un proyecto Perl y añadirlo a una aplicación.

## Procedimiento

1. En la vista Explorador, seleccione la aplicación a la que desea añadir el proyecto (si aún no ha añadido una aplicación, consulte “Configuración de aplicaciones” en la página 36).
2. Realice una de estas acciones para abrir el Asistente de proyecto nuevo:
  - a. Seleccione **Archivo > Añadir proyecto > Proyecto nuevo** en el menú principal del espacio de trabajo.
  - b. Pulse con el botón derecho en la aplicación seleccionada y elija **Añadir proyecto > Proyecto nuevo** en el menú de contexto.
3. En la página Seleccionar tipo de proyecto del asistente, seleccione **Perl** como tipo de proyecto y pulse **Siguiente** para avanzar a la siguiente página del asistente.

4. En la página del asistente de orígenes de proyecto:
  - a. Identifique los orígenes de proyecto. Los orígenes de un proyecto constan de los directorios en los que se encuentran los archivos del proyecto y de cualquier archivo individuales adicionales que se ha de incluir en el proyecto.  
Asigne un nombre al proyecto y especifique el directorio de trabajo. El **Directorio de trabajo** es la ubicación en la que residirá el archivo de proyecto de AppScan Source (.ppf). También es la base para todas las vías de acceso relativas.
  - b. Pulse **Añadir raíz del origen** para especificar una raíz del código fuente y los directorios o archivos que desea incluir en el escaneo o excluir del mismo. Después de añadir la raíz del origen, puede excluir de la misma ciertos directorios o archivos. Para ello, seleccione el directorio o archivo (o realice una selección múltiple de estos elementos) en la raíz de origen, pulse con el botón derecho en la selección y elija **Excluir** en el menú. Si incluye o excluye archivos, el icono que hay a la izquierda del nombre del archivo cambia.
5. Pulse **Finalizar**.

## Configuración de proyectos PHP

Cuando añade un nuevo proyecto PHP: Hypertext Preprocessor (PHP) a la aplicación, especifica el nombre del proyecto, va al directorio de trabajo y especifica las raíces de origen y las dependencias del proyecto. Las dependencias del proyecto también se pueden definir en el separador Dependencias del proyecto de las propiedades del proyecto después de que se cree el proyecto.

### Acerca de esta tarea

Los pasos de este tema le indican cómo completar todas las páginas del Asistente de proyecto nuevo (o el Asistente para nueva aplicación, si está creando el proyecto en el mismo). Sin embargo, algunas de las páginas del asistente son opcionales (los valores necesarios se han completado cuando el botón **Finalizar** está activado). Los valores del asistente se pueden modificar después de crear el proyecto en la vista Propiedades para un proyecto seleccionado. Si completa el Asistente de proyecto nuevo sin completar las páginas opcionales, puede cambiar los valores de estas páginas más adelante en la vista Propiedades.

**Nota:** Para PHP, VB6 y Classic ASP, sólo se da soporte a conjuntos de caracteres ISO-8859-1 (Europeo occidental), UTF-8 y UTF-16.

### Procedimiento

1. En la vista Explorador, seleccione la aplicación a la que desea añadir el proyecto (si aún no ha añadido una aplicación, consulte “Configuración de aplicaciones” en la página 36).
2. Realice una de estas acciones para abrir el Asistente de proyecto nuevo:
  - a. Seleccione **Archivo > Añadir proyecto > Proyecto nuevo** en el menú principal del espacio de trabajo.
  - b. Pulse con el botón derecho en la aplicación seleccionada y elija **Añadir proyecto > Proyecto nuevo** en el menú de contexto.
3. En la página Seleccionar tipo de proyecto del asistente, seleccione **PHP** como tipo de proyecto y pulse **Siguiente** para avanzar a la siguiente página del asistente.
4. En la página del asistente de orígenes de proyecto:

- a. Identifique los orígenes de proyecto. Los orígenes de un proyecto constan de los directorios en los que se encuentran los archivos del proyecto y de cualquier archivo individuales adicionales que se ha de incluir en el proyecto.  
Asigne un nombre al proyecto y especifique el directorio de trabajo. El **Directorio de trabajo** es la ubicación en la que residirá el archivo de proyecto de AppScan Source (.ppf). También es la base para todas las vías de acceso relativas.
- b. Pulse **Añadir raíz del origen** para especificar una raíz del código fuente y los directorios o archivos que desea incluir en el escaneo o excluir del mismo. Después de añadir la raíz del origen, puede excluir de la misma ciertos directorios o archivos. Para ello, seleccione el directorio o archivo (o realice una selección múltiple de estos elementos) en la raíz de origen, pulse con el botón derecho en la selección y elija **Excluir** en el menú. Si incluye o excluye archivos, el icono que hay a la izquierda del nombre del archivo cambia.
5. **Configuración proyecto PHP:** en el campo **Raíz de documento PHP**, especifique o vaya al directorio que representa la raíz de la aplicación PHP. Se trata del directorio del sistema de archivos que está correlacionado con la URL base del sitio. Si no se especifica ninguna raíz de documento PHP, se utiliza la raíz de origen especificada en la página Orígenes de proyecto.
6. Opcional: Defina una **Vía de acceso de inclusión**. Los directorios de vía de acceso de inclusión se utilizan para resolver vías de acceso relativas a archivos utilizados en sentencias include de PHP (por ejemplo, include, include\_once, require, require\_once).
7. Opcional: Defina una **Vía de acceso de inclusión clase**. Los directorios de las vías de acceso de inclusión de clase se utilizan para buscar archivos que contienen definiciones de clases de PHP.
8. Pulse **Finalizar**.
9. Opcional: **Configure dependencias no resueltas:** en las propiedades del proyecto, vaya a la página Dependencias del proyecto y siga los pasos de "Configuración de expresiones include de PHP no resueltas" en la página 71 y "Configuración de referencias de clase de PHP no resueltas" en la página 76.

## Ejemplo: creación de un nuevo proyecto PHP

### Acerca de esta tarea

Este ejemplo muestra cómo utilizar el Asistente para aplicaciones nuevas para crear un proyecto PHP.

### Procedimiento

1. Realice una de estas acciones:
  - Seleccione **Archivo > Añadir aplicación > Crear una nueva aplicación** en la barra del menú principal.
  - En la barra de herramientas de la vista Explorador, pulse el botón de flecha hacia abajo **Añadir menú de aplicación** y seleccione **Crear una nueva aplicación** en el menú.
  - En la vista Explorador, pulse con el botón derecho **Todas las aplicaciones** y luego seleccione **Añadir aplicación > Crear una nueva aplicación** en el menú.
2. Escriba un **Nombre** para la aplicación.
3. Vaya al **Directorio de trabajo** en el que desea guardar la aplicación. La extensión del nombre de archivo de la nueva aplicación será .paf.

4. Pulse **Siguiente** para configurar el proyecto.
5. En la página Seleccionar tipo de proyecto del asistente, seleccione **PHP** como tipo de proyecto y pulse **Siguiente** para avanzar a la siguiente página del asistente.
6. En la página Orígenes de proyecto:
  - a. En el campo **Nombre**, especifique un nombre para el proyecto; por ejemplo, MyProject.
  - b. En el campo **Directorio de trabajo**, vaya a la ubicación en la que desea almacenar el archivo de proyecto que se creará; por ejemplo, C:\Apps\MyProject.
  - c. Pulse **Añadir raíz del origen** para añadir todos los archivos que contienen archivos PHP que se deben escanear. Por ejemplo, en el cuadro de diálogo Seleccionar un archivo o directorio, vaya a C:\Apps\MyProject\root y pulse **Aceptar** para cerrar el cuadro de diálogo.

Pulse **Siguiente**.

7. En la página Configuración de proyecto PHP:
  - a. En el campo **Raíz de documento PHP**, especifique o vaya al directorio que representa la raíz de la aplicación PHP. Se trata del directorio del sistema de archivos que está correlacionado con la URL base del sitio. De forma predeterminada, este campo contiene la raíz de origen especificada en la página Orígenes de proyecto.
  - b. Opcional: Añada directorios de vías de acceso de inclusión. Se utilizan para resolver vías de acceso relativas a archivos utilizados en sentencias Include de PHP (por ejemplo, include, include\_once, require, require\_once).
  - c. Opcional: Añada directorios de vías de acceso de clase. Se utilizan para buscar archivos que contienen definiciones de clase de PHP.
8. Pulse **Finalizar**. Ya tiene un proyecto PHP preparado para que lo escanee.

## Configuración de expresiones include de PHP no resueltas

### Antes de empezar

En las propiedades del proyecto, vaya a la página Dependencias del proyecto.

### Procedimiento

1. Pulse **Configurar expresiones de inclusión no resueltas** para abrir el cuadro de diálogo Configurar expresiones de inclusión no resueltas.
2. La parte superior del cuadro de diálogo muestra las expresiones include sin resolver (todas las expresiones include que no se han resuelto o que necesitan un proceso adicional para que se resuelvan). La información proporcionada sobre las expresiones incluye:

| Opción                             | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Texto incluido / Texto actualizado | Esta columna muestra el texto de la expresión tal como aparece en el código fuente. Esta columna se puede ampliar pulsando +; se mostrará el texto actualizado que se ha utilizado durante el último escaneo. Mostrará <empty> si no había texto actualizado disponible durante el último escaneo. Es posible que se muestren varias líneas de texto actualizado cuando se amplíe; una por cada lugar del código fuente en el que se ha utilizado esta expresión.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Estado                             | Esta columna contiene una X para las expresiones que no se han resuelto o una marca de comprobación para las expresiones que se han resuelto correctamente.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Resuelto por                       | Esta columna indica cómo se ha generado el texto actualizado. Los valores incluyen: <ul style="list-style-type: none"> <li>• AutoResolver: la aplicación ha utilizado la heurística interna para buscar el archivo.</li> <li>• SearchReplace: se han aplicado una o varias reglas de búsqueda y sustitución al texto incluido para generar el texto actualizado.</li> <li>• SearchReplace+AutoResolver: se han aplicado una o varias reglas de búsqueda y sustitución al texto incluido para generar el texto actualizado y luego se ha aplicado heurística interna para encontrar el archivo.</li> <li>• SearchReplace+IncludePath: se han aplicado una o varias reglas de búsqueda y sustitución al texto incluido para generar el texto actualizado y luego se ha combinado con un directorio de la vía de acceso de inclusión para buscar el archivo.</li> <li>• SearchReplace+RelativeDir: se han aplicado una o varias reglas de búsqueda y sustitución al texto incluido para generar el texto actualizado y luego se ha encontrado en relación con el directorio de origen del archivo que contiene la expresión include</li> </ul> |
| Archivo de origen, línea, columna  | Estas columnas muestran la ubicación en el código fuente en la que se ha utilizado la expresión. Es posible que desee examinar estas ubicaciones en un editor para ver cómo se deben resolver.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

**Nota:** Puede que algunas de las columnas estén en blanco. Esto se debe a que el texto puede tener varias líneas de texto actualizado cuando se amplía. Estas columnas tendrán el texto adecuado para cada una de estas líneas de texto actualizado.



3. En la parte inferior del cuadro de diálogo, el separador Vía de acceso de inclusión contiene la información sobre la vía de acceso de inclusión que se ha especificado en la página Dependencias del proyecto PHP. Puede actualizar esta información en el cuadro de diálogo (mientras visualiza las expresiones incluye no resueltas).
4. En la parte inferior del cuadro de diálogo, el separador Buscar y sustituir se utiliza para añadir reglas para sustituir texto dinámico en una expresión incluye por texto estático que constituye una vía de acceso a archivo completa o parcial a un archivo incluye. La tabla Buscar y sustituir contiene tres columnas:

| Opción                   | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Mandato</b>           | <p>El valor de esta columna determina el modo en que se utilizan las columnas <b>Texto de búsqueda</b> y <b>Texto de sustitución</b>. Las opciones son:</p> <ul style="list-style-type: none"> <li>• <b>Sustituir texto:</b> este mandato sirve para realizar búsquedas y sustituciones de texto simple. El <b>Texto de búsqueda</b> se utiliza tal cual y, si se encuentra en algún lugar en el texto incluido, se sustituye por el <b>Texto de sustitución</b>.</li> <li>• <b>Sustituir función:</b> este mandato se utiliza cuando hay que sustituir una llamada de función. El <b>Texto de búsqueda</b> debe ser el nombre de la función sin paréntesis. El texto de búsqueda se aumentará para buscar una llamada de función con el nombre especificado seguido de paréntesis y coincidirá con cualquier texto que esté entre paréntesis.</li> <li>• <b>Sustituir expresión regular:</b> es una característica avanzada que permite especificar una expresión regular para el texto de búsqueda.</li> </ul> |
| <b>Texto de búsqueda</b> | <p>Es el texto que hay que buscar en la expresión incluye. Puede seleccionar texto dentro de una expresión incluye, copiarlo en el portapapeles y pegarlo aquí. Consulte la descripción anterior de la columna <b>Mandato</b> para ver las variaciones al especificar el texto de búsqueda.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| Opción               | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Texto de sustitución | <p>Es el texto utilizado para sustituir el texto de búsqueda. Se trata de texto estático que constituye una vía de acceso a archivo completa o parcial a un archivo <code>include</code>. También hay algunas variables que se pueden colocar en el texto de sustitución. Se pueden escribir directamente en la celda <b>Texto de sustitución</b> o se pueden seleccionar en el menú <b>Variables de texto de sustitución</b> que hay sobre la tabla (se copiará la variable seleccionada en el portapapeles). Las variables que se pueden seleccionar en la lista de menú <b>Variables de texto de sustitución</b> son:</p> <ul style="list-style-type: none"> <li>• <code>%ROOT_DIR%</code>: esta variable se sustituirá por el directorio raíz del documento PHP especificado para el proyecto.</li> <li>• <code>%SRC_DIR%</code>: esta variable se sustituirá por el directorio del archivo que contiene la expresión <code>include</code>.</li> <li>• <code>%ARG_N%</code>: esta variable solo se aplica cuando el mandato es <b>Sustituir función</b>. N en la variable se debe sustituir por un entero (por ejemplo, <code>%ARG_1%</code> o <code>%ARG_2%</code>). Luego esta variable se sustituirá por el texto que se pasa en el parámetro número N de la llamada de función.</li> </ul> |

Las reglas se aplican en orden. Tras una operación correcta de búsqueda y sustitución, se comprueba el nuevo texto para ver si se encuentra el archivo. Si el archivo no se encuentra, se prueba la siguiente regla sobre el texto actualizado.

Cada proyecto PHP empieza por tres reglas de búsqueda y sustitución que intentan sustituir algunas constantes y funciones estándares de PHP que se suelen utilizar en expresiones `include`.

#### Ejemplo: configuración de expresiones `include` no resueltas: Antes de empezar

Las expresiones `include` no resueltas se configuran en la página con separadores Dependencias del proyecto de las propiedades del proyecto. Cuando esté en la página, pulse **Configurar expresiones de inclusión no resueltas** para abrir el cuadro de diálogo Configurar expresiones de inclusión no resueltas.

En este ejemplo se da por supuesto que ha añadido una vía de acceso de inclusión al proyecto (esto se puede hacer al crear el proyecto o desde la página Dependencias del proyecto) y que ha ejecutando un escaneo. Una vez finalizada el escaneo, abra el cuadro de diálogo Configurar expresiones de inclusión no resueltas para ver la lista **Expresiones de inclusión no resueltas**. En este ejemplo, `MYPROJECT_ROOT_PATH.'/a/b/filename.php'`, `MYPROJECT_ROOT_PATH.'/language/'`, `'.$configInfo['language'].'/mypage.php'`, y `configGet('database_inc','./includes/database.inc')` son expresiones de dicha lista.

## Procedimiento

1. Sustituya una constante o variable de PHP inicial por un directorio siguiendo estos pasos:
  - a. Seleccione MYPROJECT\_ROOT\_PATH. '/a/b/filename.php' - esto hace que se seleccione el texto de la expresión. Luego puede utilizar el ratón o las teclas del cursor para seleccionar una parte de la expresión. Seleccione MYPROJECT\_ROOT\_PATH y pulse con el botón derecho del ratón y seleccione **Copiar**.
  - b. Seleccione el separador Buscar y sustituir.
  - c. Pulse el botón **Añadir regla para el elemento no resuelto seleccionado** (contiene un símbolo **más** verde). Esto añade una nueva regla de búsqueda y sustitución a la lista.
  - d. En la nueva regla, seleccione NewSearchText y pulse con el botón derecho y seleccione **Pegar** en el menú. Esto hace que NewSearchText se sustituya por MYPROJECT\_ROOT\_PATH.
  - e. En el menú **Variables de texto de sustitución**, seleccione %ROOT\_DIR%. Esto hace que la serie de texto %ROOT\_DIR% se copie en el portapapeles.
  - f. En la regla, seleccione NewReplacementText y pulse con el botón derecho y seleccione **Pegar** en el menú. Esto hace que NewReplacementText se sustituya por %ROOT\_DIR%.

Ahora tiene una nueva regla que correlacionará una constante con la vía de acceso al directorio raíz del documento PHP. El operador de concatenación PHP (.) y la serie de texto que sigue se combinarán con el texto de sustitución para generar una expresión de vía de acceso individual. La próxima vez que se escanee el proyecto, las expresiones incluye que utilicen esta constante deberían ejecutarse correctamente.

2. Para sustituir una expresión dinámica por un solo valor:
  - a. Seleccione MYPROJECT\_ROOT\_PATH. '/language/' . \$configInfo['language'] . '/mypage.php' - esto hace que se seleccione el texto de la expresión. Luego puede utilizar el ratón o las teclas del cursor para seleccionar una parte de la expresión. Seleccione \$configInfo['language'] y pulse con el botón derecho del ratón y seleccione **Copiar**.
  - b. Seleccione el separador Buscar y sustituir.
  - c. Pulse el botón **Añadir regla para el elemento no resuelto seleccionado** (contiene un símbolo **más** verde). Esto añade una nueva regla de búsqueda y sustitución a la lista.
  - d. En la nueva regla, seleccione NewSearchText y pulse con el botón derecho y seleccione **Pegar** en el menú. Esto hace que NewSearchText se sustituya por \$configInfo['language'].
  - e. En la regla, seleccione NewReplacementText y sustitúyalo por el nuevo texto escribiendo english.

Ahora tiene una nueva regla que sustituirá la expresión por el valor especificado. El operador de concatenación de PHP (.) se aplicará para generar una sola expresión de vía de acceso. La próxima vez que se escanee el proyecto, las expresiones incluye que utilicen esta expresión deberían ejecutarse correctamente.

3. Para sustituir una llamada de función de PHP por uno de sus argumentos:
  - a. Seleccione configGet('database\_inc', './includes/database.inc') - esto hace que se seleccione el texto de la expresión. Luego puede utilizar el ratón o las teclas del cursor para seleccionar una parte de la expresión. Seleccione configGet y pulse con el botón derecho del ratón y seleccione **Copiar**.

- b. Seleccione el separador **Buscar y sustituir**.
- c. En la nueva regla, seleccione **Sustituir texto** en la primera columna y luego seleccione **Sustituir función** en el menú.
- d. En la regla, seleccione **NewSearchText** y pulse con el botón derecho y seleccione **Pegar** en el menú. Esto hace que **NewSearchText** se sustituya por **configGet**.
- e. En el menú **Variables de texto de sustitución**, seleccione **%ARG\_1%**. Esto hace que la variable se copie en el portapapeles.
- f. En la regla, seleccione **NewReplacementText** y pulse con el botón derecho y seleccione **Pegar** en el menú. Edite el texto pegado y especifique **%ARG\_2%** en lugar de **%ARG\_1%**.

Ahora tiene una nueva regla que sustituirá una llamada de función por el valor de su segundo parámetro. La próxima vez que se escanee el proyecto, las expresiones **include** que utilicen esta llamada de función deberían ejecutarse correctamente.

## Configuración de referencias de clase de PHP no resueltas

### Antes de empezar

En las propiedades del proyecto, vaya a la página **Dependencias del proyecto**.

### Procedimiento

1. Pulse **Configurar referencias de clase no resueltas** para abrir el cuadro de diálogo **Configurar referencias de clase no resueltas**.
2. La parte superior del cuadro de diálogo contiene las referencias de clase no resueltas (todas las referencias de clase que no se han resuelto durante el último escaneo). La información proporcionada sobre las referencias de clase incluye:

| Opción                                              | Descripción                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Nombre de clase / Nombre de archivo generado</b> | Esta columna muestra el nombre de clase al que se hace referencia en el código fuente. Esta columna se puede ampliar pulsando <b>+</b> ; se mostrará el nombre de archivo generado que se ha utilizado durante el último escaneo para probar y buscar la clase. Es posible que aparezcan varios nombres de archivo cuando se amplíe; uno por cada lugar del código fuente en el que se ha utilizado esta clase. |
| <b>Estado</b>                                       | Esta columna contiene una <b>X</b> para las clases que no se han resuelto o una marca de comprobación para las clases que se han resuelto correctamente.                                                                                                                                                                                                                                                        |
| <b>Resuelto por</b>                                 | Esta columna indica cómo se ha creado el nombre de archivo generado. Los valores incluyen: <ul style="list-style-type: none"> <li>• <b>AutoResolver</b>: la aplicación ha utilizado la heurística interna para buscar el archivo.</li> <li>• <b>SearchReplace</b>: se han aplicado una o varias reglas de búsqueda y sustitución al nombre de clase para crear el nombre de archivo generado.</li> </ul>        |

| Opción                            | Descripción                                                                                                                                                                                |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Archivo de origen, línea, columna | Estas columnas muestran la ubicación en el código fuente en la que se ha utilizado la clase. Es posible que desee examinar estas ubicaciones en un editor para ver cómo se deben resolver. |

**Nota:** Puede que algunas de las columnas estén en blanco. Esto se debe a que los nombres de clase pueden generar varias líneas de nombre de archivo generado cuando se amplían. Estas columnas tendrán el texto adecuado para cada una de estas líneas de nombre de archivo generado.

3. En la parte inferior del cuadro de diálogo, el separador Vía de acceso de inclusión clase contiene la información sobre la vía de acceso de inclusión de clase que se ha especificado en la página Dependencias del proyecto PHP. Puede actualizar esta información en el cuadro de diálogo (mientras consulta las referencias de clase no resueltas).
4. En la parte inferior del cuadro de diálogo, se utiliza el separador Buscar y sustituir para añadir reglas para cambiar el nombre de clase no resuelto por una vía de acceso a archivo completa o parcial que contenga la definición de dicha clase. La tabla Buscar y sustituir contiene tres columnas:

| Opción  | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mandato | <p>El valor de esta columna determina el modo en que se utilizan las columnas <b>Texto de búsqueda</b> y <b>Texto de sustitución</b>. Las opciones son:</p> <ul style="list-style-type: none"> <li>• <b>Comparar texto:</b> este comando se utiliza para buscar y sustituir texto. Se permite el carácter * en el texto de búsqueda, que puede coincidir con 0 o más caracteres. El resultado de una comparación de texto no afecta a ninguna otra regla de búsqueda y sustitución. Suele utilizarse para intentar añadir una extensión al nombre de clase o para filtrar los prefijos y sufijos del nombre de clase cuando se genera un nombre de archivo.</li> <li>• <b>Sustituir texto:</b> este mandato sirve para realizar búsquedas y sustituciones de texto simple. El <b>Texto de búsqueda</b> se utiliza tal cual y, si se encuentra en algún lugar del nombre de clase, se sustituye por el <b>Texto de sustitución</b>. Se utiliza para modificar el nombre de clase para utilizarlo en las siguientes reglas.</li> <li>• <b>Sustituir expresión regular:</b> es una característica avanzada que permite especificar una expresión regular para el texto de búsqueda.</li> </ul> |

| Opción               | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Texto de búsqueda    | Es el texto que hay que buscar en la referencia de clase. Puede seleccionar texto dentro de un nombre de clase, copiarlo en el portapapeles y pegarlo aquí. Consulte la descripción anterior de la columna <b>Mandato</b> para ver las variaciones al especificar el texto de búsqueda.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Texto de sustitución | <p>Es el texto utilizado para sustituir el texto de búsqueda. Se trata de texto estático que constituye una vía de acceso completa o parcial a un archivo que contiene la definición de la clase. También hay algunas variables que se pueden colocar en el texto de sustitución. Se pueden escribir directamente en la celda <b>Texto de sustitución</b> o se pueden seleccionar en el menú <b>Variables de texto de sustitución</b> que hay sobre la tabla (se copiará la variable seleccionada en el portapapeles). Las variables que se pueden seleccionar en la lista de menú <b>Variables de texto de sustitución</b> son:</p> <ul style="list-style-type: none"> <li>• %ROOT_DIR%: esta variable se sustituirá por el directorio raíz del documento PHP especificado para el proyecto.</li> <li>• %SRC_DIR%: esta variable se sustituirá por el directorio del archivo que contiene la referencia a la clase.</li> <li>• %MATCH_N%: esta variable solo se aplica cuando el mandato es <b>Comparar texto</b>. N en la variable se debe sustituir por un entero (por ejemplo, %MATCH_1% o %MATCH_2%). Luego esta variable se sustituirá por el texto que coincida con el carácter * número N en el texto de búsqueda.</li> </ul> |

Las reglas se aplican en orden. Tras una operación correcta de búsqueda y sustitución, se comprueba el nuevo texto para ver si se encuentra el archivo. Si el archivo no se encuentra, se prueba la siguiente regla sobre el texto actualizado, excepto si el mandato es **Comparar texto**.

Cada proyecto PHP comienza por dos reglas de búsqueda y sustitución simples que intentan añadir algunas extensiones de archivo comunes al nombre de clase.

5. En la parte inferior del cuadro de diálogo, el separador Clases encontradas lista todas las clases que se han encontrado durante el último escaneo. Esto se puede utilizar para actualizar la vía de acceso de inclusión de la clase y reglas de búsqueda y sustitución. Puede seleccionar una referencia de clase no resuelta en la sección Referencias de clase no resueltas del diálogo y pulsar **Buscar declaración**. Si se encuentra la declaración, se muestra en la lista del separador Clases encontradas.

**Ejemplo: configuración de referencias de clase no resueltas:**

## Antes de empezar

Las referencias de clase no resueltas se configuran en la página con separadores Dependencias del proyecto de las propiedades del proyecto. Cuando esté en la página, pulse **Configurar referencias de clase no resueltas** para abrir el cuadro de diálogo Configurar referencias de clase no resueltas.

En este ejemplo se da por supuesto que ha añadido una vía de acceso de inclusión de clase al proyecto (esto se puede hacer al crear el proyecto o desde la página Dependencias del proyecto) y que ha ejecutando un escaneo. Una vez finalizada el escaneo, abra el cuadro de diálogo Configurar referencias de clase no resueltas para ver la lista **Referencias de clase no resueltas**.

En estos ejemplos, se proporcionan valores de texto de sustitución. Observe que puede haber varias variables en el texto; por ejemplo, `%ROOT_DIR%/modules/%MATCH_1%/classes/%MATCH_1%.class.inc`.

## Procedimiento

1. Para añadir otra extensión de archivo utilizada por los archivos include:
  - a. Seleccione el separador Buscar y sustituir.
  - b. Pulse el botón **Añadir regla para el elemento no resuelto seleccionado** (contiene un símbolo **más** verde). Esto añade una nueva regla de búsqueda y sustitución a la lista.
  - c. En la nueva regla, seleccione el **Texto de sustitución**, `%MATCH_1%.php`. En esta serie, suprima `.php` y escriba `.class.inc` en su lugar. Ahora el **Texto de sustitución** debería ser `%MATCH_1%.class.inc`.

Ahora tiene una nueva regla que intentará añadir el sufijo `.class.inc` a un nombre de clase cuando resuelva la clase.

2. Para eliminar un prefijo de un nombre de clase:
  - a. Seleccione el separador Buscar y sustituir.
  - b. Pulse el botón **Añadir regla para el elemento no resuelto seleccionado** (contiene un símbolo **más** verde). Esto añade una nueva regla de búsqueda y sustitución a la lista.
  - c. En la nueva regla, seleccione la serie de la columna **Texto de búsqueda (\*)** y escriba `Abc*` en su lugar.
  - d. No modifique el texto de sustitución `%MATCH_1%.php`.

Ahora tiene una nueva regla que correlacionará nombres de clase como `AbcHello` con `Hello.php`.

3. Para eliminar un sufijo de un nombre de clase:
  - a. Seleccione el separador Buscar y sustituir.
  - b. Pulse el botón **Añadir regla para el elemento no resuelto seleccionado** (contiene un símbolo **más** verde). Esto añade una nueva regla de búsqueda y sustitución a la lista.
  - c. En la nueva regla, seleccione la serie de la columna **Texto de búsqueda (\*)** y escriba `*Xyz` en su lugar.
  - d. No modifique el texto de sustitución `%MATCH_1%.php`.

Ahora tiene una nueva regla que correlacionará nombres de clase como `ByeByeXyz` con `ByeBye.php`.

4. Es posible que desee correlacionar nombres de clase como `Abc_Def_Ghi_class` de modo que sus prefijos se utilicen como vías de acceso relativas en el sistema

de archivos (por ejemplo `Abc/Def/Ghi/class.php`). Para modificar el texto de un nombre de clase para utilizarlo en otras reglas:

- a. Seleccione el separador **Buscar y sustituir**.
- b. Pulse el botón **Añadir regla para el elemento no resuelto seleccionado** (contiene un símbolo **más** verde). Esto añade una nueva regla de búsqueda y sustitución a la lista.
- c. En la nueva regla, seleccione **Comparar texto** en la primera columna y luego seleccione **Sustituir texto** en el menú.
- d. En la regla, seleccione la serie de la columna **Texto de búsqueda (\*)** y escriba `_` en su lugar.
- e. Seleccione la serie en la columna **Texto de sustitución** y escriba `/` en su lugar.
- f. Mientras la regla esté seleccionada, seleccione **Mover arriba** para mover esta regla al principio de la lista.

Ahora tiene una nueva regla que sustituirá los signos de subrayado (`_`) por barras inclinadas (`/`) y las siguientes reglas utilizarán el texto actualizado. Esta regla cambiará `Abc_Def_Ghi_class` por `Abc/Def/Ghi/class` y las restantes reglas de **Comparar texto** intentarán añadir extensiones, como `.php` y `.inc`.

## Adición de un nuevo proyecto PL/SQL

El Asistente de nuevo proyecto le ayuda a crear manualmente un proyecto PL/SQL y añadirlo a una aplicación.

### Acerca de esta tarea

Los pasos de este tema le indican cómo completar todas las páginas del Asistente de proyecto nuevo (o el Asistente para nueva aplicación, si está creando el proyecto en el mismo). Los valores del asistente se pueden modificar después de crear el proyecto en la vista Propiedades para un proyecto seleccionado.

### Procedimiento

1. En la vista Explorador, seleccione la aplicación a la que desea añadir el proyecto (si aún no ha añadido una aplicación, consulte “Configuración de aplicaciones” en la página 36).
2. Realice una de estas acciones para abrir el Asistente de proyecto nuevo:
  - a. Seleccione **Archivo > Añadir proyecto > Proyecto nuevo** en el menú principal del espacio de trabajo.
  - b. Pulse con el botón derecho en la aplicación seleccionada y elija **Añadir proyecto > Proyecto nuevo** en el menú de contexto.
3. En la página Seleccionar tipo de proyecto del asistente, seleccione **PL/SQL** como tipo de proyecto y pulse **Siguiente** para avanzar a la siguiente página del asistente.
4. En la página del asistente de orígenes de proyecto:
  - a. Identifique los orígenes de proyecto. Los orígenes de un proyecto constan de los directorios en los que se encuentran los archivos del proyecto y de cualquier archivo individuales adicionales que se ha de incluir en el proyecto.  
Asigne un nombre al proyecto y especifique el directorio de trabajo. El **Directorio de trabajo** es la ubicación en la que residirá el archivo de proyecto de AppScan Source (`.ppf`). También es la base para todas las vías de acceso relativas.



- b. Pulse **Añadir raíz del origen** para especificar una raíz del código fuente y los directorios o archivos que desea incluir en el escaneo o excluir del mismo. Después de añadir la raíz del origen, puede excluir de la misma ciertos directorios o archivos. Para ello, seleccione el directorio o archivo (o realice una selección múltiple de estos elementos) en la raíz de origen, pulse con el botón derecho en la selección y elija **Excluir** en el menú. Si incluye o excluye archivos, el icono que hay a la izquierda del nombre del archivo cambia.
5. Pulse **Finalizar**.

## Adición de un nuevo proyecto T-SQL

El Asistente de nuevo proyecto le ayuda a crear manualmente un proyecto T-SQL y a añadirlo a una aplicación.

### Acerca de esta tarea

Los pasos de este tema le indican cómo completar todas las páginas del Asistente de proyecto nuevo (o el Asistente para nueva aplicación, si está creando el proyecto en el mismo). Los valores del asistente se pueden modificar después de crear el proyecto en la vista Propiedades para un proyecto seleccionado.

### Procedimiento

1. En la vista Explorador, seleccione la aplicación a la que desea añadir el proyecto (si aún no ha añadido una aplicación, consulte “Configuración de aplicaciones” en la página 36).
2. Realice una de estas acciones para abrir el Asistente de proyecto nuevo:
  - a. Seleccione **Archivo > Añadir proyecto > Proyecto nuevo** en el menú principal del espacio de trabajo.
  - b. Pulse con el botón derecho en la aplicación seleccionada y elija **Añadir proyecto > Proyecto nuevo** en el menú de contexto.
3. En la página Seleccionar tipo de proyecto del asistente, seleccione **T-SQL** como tipo de proyecto y pulse **Siguiente** para avanzar a la siguiente página del asistente.
4. En la página del asistente de orígenes de proyecto:
  - a. Identifique los orígenes de proyecto. Los orígenes de un proyecto constan de los directorios en los que se encuentran los archivos del proyecto y de cualquier archivo individuales adicionales que se ha de incluir en el proyecto.  
Asigne un nombre al proyecto y especifique el directorio de trabajo. El **Directorio de trabajo** es la ubicación en la que residirá el archivo de proyecto de AppScan Source (.ppf). También es la base para todas las vías de acceso relativas.
  - b. Pulse **Añadir raíz del origen** para especificar una raíz del código fuente y los directorios o archivos que desea incluir en el escaneo o excluir del mismo. Después de añadir la raíz del origen, puede excluir de la misma ciertos directorios o archivos. Para ello, seleccione el directorio o archivo (o realice una selección múltiple de estos elementos) en la raíz de origen, pulse con el botón derecho en la selección y elija **Excluir** en el menú. Si incluye o excluye archivos, el icono que hay a la izquierda del nombre del archivo cambia.
5. Pulse **Finalizar**.

# Adición de un nuevo proyecto Visual Basic

## Acerca de esta tarea

**Nota:** Este tipo de proyecto está soportado sólo en Windows.

Los pasos de este tema le indican cómo completar todas las páginas del Asistente de proyecto nuevo (o el Asistente para nueva aplicación, si está creando el proyecto en el mismo). Los valores del asistente se pueden modificar después de crear el proyecto en la vista Propiedades para un proyecto seleccionado.

**Nota:** Para PHP, VB6 y Classic ASP, sólo se da soporte a conjuntos de caracteres ISO-8859-1 (Europeo occidental), UTF-8 y UTF-16.

## Procedimiento

1. En la vista Explorador, seleccione la aplicación a la que desea añadir el proyecto (si aún no ha añadido una aplicación, consulte “Configuración de aplicaciones” en la página 36).
2. Realice una de estas acciones para abrir el Asistente de proyecto nuevo:
  - a. Seleccione **Archivo > Añadir proyecto > Proyecto nuevo** en el menú principal del espacio de trabajo.
  - b. Pulse con el botón derecho en la aplicación seleccionada y elija **Añadir proyecto > Proyecto nuevo** en el menú de contexto.
3. En la página Seleccionar tipo de proyecto del asistente, seleccione **Visual Basic** como tipo de proyecto y pulse **Siguiente** para pasar a la siguiente página del asistente.
4. En la página del asistente de orígenes de proyecto:
  - a. Identifique los orígenes de proyecto. Los orígenes de un proyecto constan de los directorios en los que se encuentran los archivos del proyecto y de cualquier archivo individuales adicionales que se ha de incluir en el proyecto.  
Asigne un nombre al proyecto y especifique el directorio de trabajo. El **Directorio de trabajo** es la ubicación en la que residirá el archivo de proyecto de AppScan Source (.ppf). También es la base para todas las vías de acceso relativas.
  - b. Pulse **Añadir raíz del origen** para especificar una raíz del código fuente y los directorios o archivos que desea incluir en el escaneo o excluir del mismo. Después de añadir la raíz del origen, puede excluir de la misma ciertos directorios o archivos. Para ello, seleccione el directorio o archivo (o realice una selección múltiple de estos elementos) en la raíz de origen, pulse con el botón derecho en la selección y elija **Excluir** en el menú. Si incluye o excluye archivos, el icono que hay a la izquierda del nombre del archivo cambia.
5. Pulse **Finalizar**.

---

## Cómo copiar proyectos

AppScan Source for Analysis permite copiar todos los tipos de proyecto excepto los proyectos .NET. Las modificaciones en el proyecto no afectan al proyecto duplicado; después de copiar un proyecto, no hay ninguna conexión entre el proyecto original y el copiado. Cuando copia un proyecto importado, se crea un archivo de proyecto AppScan Source (.ppf) con toda la información sobre la configuración.

## Procedimiento

1. En la vista Explorador, pulse con el botón derecho en el proyecto que desea copiar y seleccione **Copiar proyecto** en el menú.
2. En el cuadro de diálogo Copiar proyecto:
  - a. Asigne un nombre al nuevo proyecto.
  - b. Identifique la aplicación de destino para el proyecto duplicado (la aplicación de destino debe ser una aplicación de AppScan Source creada manualmente o utilizando Application Discovery Assistant).
  - c. Identifique un directorio de destino (directorio de trabajo del proyecto copiado).

---

## Modificación de las propiedades del proyecto y de la aplicación

Cuando selecciona una aplicación o un proyecto en la vista Explorador, las propiedades actuales aparecen en la vista Propiedades, donde puede realizar modificaciones.

### Acerca de esta tarea

“Vista Propiedades: aplicación seleccionada” en la página 258 y “Vista Propiedades: proyecto seleccionado” en la página 259 proporcionan información detallada acerca de los valores que se pueden modificar en la vista Propiedades cuando se selecciona una aplicación o proyecto.

## Procedimiento

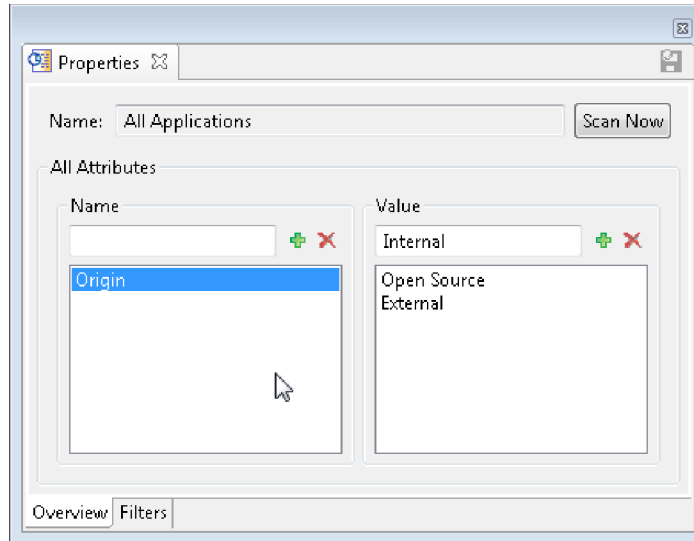
1. Abra la vista Propiedades de la aplicación o proyecto que utilice uno de estos métodos:
  - a. Seleccione la aplicación o el proyecto en la vista Explorador y, a continuación, abra la vista Propiedades para que se muestren las propiedades.
  - b. Pulse con el botón derecho sobre la aplicación o el proyecto en la vista Explorador y seleccione **Propiedades**.
2. Revise las propiedades en la vista Propiedades.
3. Realice los cambios en las páginas de los separadores adecuados. Las páginas de propiedades disponibles dependen del idioma.
4. Pulse **Guardar**.

---

## Atributos globales

Los atributos globales deben definirse antes de poder asociarlos a aplicaciones individuales. Los atributos globales se definen en la vista Propiedades seleccionando **Todas las aplicaciones** en la vista Explorador.

## Acerca de esta tarea



Para suprimir un atributo o su valor, seleccione el nombre o el valor y pulse **Suprimir atributo** (✖). El hecho de suprimir un atributo no afecta a los resultados históricos.

Para crear un atributo y hacer que esté disponible para cualquier aplicación:

### Procedimiento

1. Seleccione **Todas las aplicaciones** en la vista Explorador.
2. Abra el separador **Visión general** en la vista Propiedades.
3. Escriba un nombre para el atributo y pulse **Añadir atributo** (+) o pulse **Añadir atributo** sin especificar un nombre (se le solicitará mediante un cuadro de diálogo que especifique un nombre para el atributo).
4. Escriba un **Valor** para el atributo y pulse **Añadir valor de atributo** o pulse **Añadir valor de atributo** sin especificar un primer valor (se le solicitará mediante un cuadro de diálogo que añada un valor).
5. Repita estos pasos para añadir varios valores de atributo.

---

## Atributos de aplicación

Los atributos de aplicación se aplican a la aplicación actualmente seleccionada y dependen de atributos globales creados previamente.

### Procedimiento

1. Seleccione la aplicación en la vista Explorador.
2. Abra el separador **Visión general** en la vista Propiedades.
3. Pulse **Añadir atributos**. El cuadro de diálogo **Atributos globales** aparece con una lista de atributos creada previamente (las instrucciones para crear atributos globales se encuentran en “Atributos globales” en la página 83).
4. Pulse dos veces el atributo que desee añadir o selecciónelo y pulse **Aceptar**. El atributo se añade a la sección Atributos de aplicación de la vista Propiedades.

5. Pulse la columna **Valor** y seleccione un valor para esta aplicación en la lista (hay varios valores disponibles si el atributo global se ha creado con varios valores). Puede asociar varios atributos a una aplicación.

---

## Eliminación de aplicaciones y proyectos

Puede eliminar aplicaciones y proyectos de AppScan Source for Analysis si no están registrados.

### Procedimiento

1. Seleccione una aplicación o un proyecto que desee eliminar. Se pueden seleccionar varias aplicaciones y proyectos para eliminarlos. Sin embargo, no se puede seleccionar una mezcla de aplicaciones y proyectos para eliminarla.
2. Realice una de estas acciones:
  - Pulse con el botón derecho en la selección y elija **Eliminar aplicación** o **Eliminar proyecto** del menú.
  - Pulse la tecla Suprimir del teclado.
  - Seleccione **Editar > Eliminar** en el menú principal del espacio de trabajo.

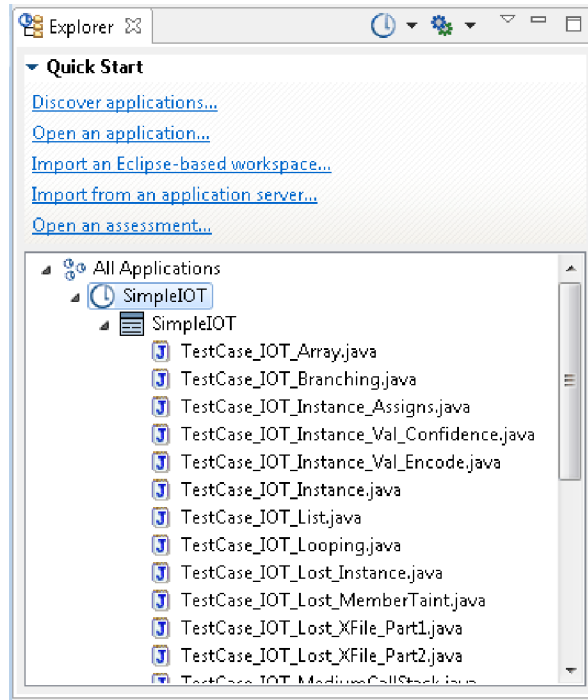
---

## Vista Explorador

La vista Explorador contiene una sección **Inicio rápido** en la parte superior y una sección Explorador en la parte inferior que contiene un nodo, **Todas las aplicaciones**. La sección **Inicio rápido** sección contiene varios enlaces útiles que inician acciones comunes. La sección Explorador está formada por un panel de árbol que ofrece una vista jerárquica de los recursos: aplicaciones, proyectos, directorios y archivos de proyecto, con **Todas las aplicaciones** como raíz. Puede navegar por estos recursos como si estuviera en un navegador de archivos. A medida que navega por la vista, el estado de selección del árbol determina los separadores disponibles en la vista Propiedades.

- “Información general” en la página 86
- “Sección Inicio rápido” en la página 86
- “Botones de la barra de herramientas” en la página 87
- “Opciones del menú del botón derecho ” en la página 88
- “Indicadores de aplicaciones y proyectos ” en la página 90

## Información general



En la vista Explorador, puede añadir aplicaciones y proyectos, y escanear código utilizando los botones de la barra de herramienta, los enlaces en la sección **Inicio rápido** o los mandatos del menú que aparecen al pulsar con el botón derecho en la sección Explorador. Una vez añadidas las aplicaciones, la sección Explorador ofrece indicadores visuales de las aplicaciones y proyectos y del estado de cada uno de ellos.

**Consejo:** En la vista Explorador, la ayuda contextual está disponible para indicar el nombre del archivo y vía de acceso de aplicaciones, proyectos y archivos. La ayuda contextual también indica si una aplicación o proyecto están registrados.

### Sección Inicio rápido

La sección **Inicio rápido** ofrece estos enlaces para iniciar tareas comunes:

- **Descubrir aplicaciones:** Esto inicia Application Discovery Assistant, que permite crear y configurar aplicaciones y proyectos con rapidez para código fuente Java y Microsoft Visual Studio
- **Abrir una aplicación:** Inicia un cuadro de diálogo Abrir, que permite examinar y buscar un y añadir una aplicación existente al conjunto de aplicaciones. Los tipos de archivos o directorios que se pueden añadir son `.paf`, `.sln`, `.dsw` y `.ewf`.
- **Importar un espacio de trabajo basado en Eclipse:** Inicia el cuadro de diálogo Añadir espacio de trabajo, que permite añadir un espacio de trabajo Eclipse o IBM Rational Application Developer for WebSphere Software (RAD) existente que contiene proyectos Java. Una vez importado el espacio de trabajo, podrá escanear los proyectos Java que contiene.

**Nota:** Antes de importar un espacio de trabajo, asegúrese de haber instalado y actualizado el entorno de desarrollo tal como se describe en “Configuración del

entorno de desarrollo para proyectos de Eclipse y Rational Application Developer for WebSphere Software (RAD)” en la página 47.

- **Importar desde un servidor de aplicaciones:** Importar una aplicación Java existente desde un servidor de aplicaciones Apache Tomcat o WebSphere Application Server Liberty.
- **Abrir un asesoramiento:** Inicia un cuadro de diálogo Abrir, que permite examinar y buscar un archivo de asesoramiento de AppScan Source. Los tipos de archivo que se pueden abrir son .ozasmt y .xml.

## Botones de la barra de herramientas

Tabla 8. Botones de la barra de herramientas

| Acción                    | Icono                                                                             | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Añadir menú de aplicación |  | Cuando pulsa la flecha hacia abajo en el botón <b>Añadir menú de aplicación</b> , puede seleccionar acciones para crear una nueva aplicación, abrir una aplicación existente, importar un espacio de trabajo o iniciar Application Discovery Assistant.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Escanear selección        |  | El botón <b>Escanear selección</b> permite escanear el objeto que se ha seleccionado en la sección Explorador. Se utilizará la configuración de escaneo predeterminada para el escaneo. Para elegir otra configuración del escaneo que se utilizará para el escaneo, pulse la flecha hacia abajo en el botón <b>Escanear selección</b> . Seleccione la configuración de escaneo que desee utilizar. O bien, seleccione la acción <b>Editar configuraciones</b> para establecer una configuración de escaneo diferente como valor predeterminado (en la vista Configuración del escaneo, seleccione la configuración que desea establecer como valor predeterminado y, a continuación, pulse <b>Seleccionar como valor predeterminado</b> ). |
| Menú Ver                  |                                                                                   | El botón <b>Menú Ver</b> abre un menú que permite renovar la sección Explorador y ocultar los elementos registrados.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## Opciones del menú del botón derecho

La disponibilidad de las opciones del menú que aparece al pulsar el botón derecho del ratón están determinadas por el elemento seleccionado en la sección Explorador.

- Al seleccionar **Todas las aplicaciones** en la sección Explorador, estas opciones del menú que aparece al pulsar el botón derecho del ratón están disponibles:
  - **Escanear todas las aplicaciones:** Escanea todas las aplicaciones. El escaneo se ejecutará con la configuración de escaneo predeterminada.
  - **Escanear todas las aplicaciones con:** Seleccione la configuración de escaneo que desee utilizar. O bien, seleccione la acción **Editar configuraciones** para establecer una configuración de escaneo diferente como valor predeterminado (en la vista Configuración del escaneo, seleccione la configuración que desea establecer como valor predeterminado y, a continuación, pulse **Seleccionar como valor predeterminado**).
  - **Añadir aplicación**
    - **Crear una nueva aplicación:** Añadir una nueva aplicación al conjunto de aplicaciones. Esta acción inicia el Asistente para aplicaciones nuevas.
    - **Abrir una aplicación existente:** Inicia un cuadro de diálogo Abrir, que permite examinar y buscar un y añadir una aplicación existente al conjunto de aplicaciones. Los tipos de archivos o directorios que se pueden añadir son .paf,.sln, .dsw y .ewf.
    - **Importar un espacio de trabajo basado en Eclipse existente:** Inicia el cuadro de diálogo Añadir espacio de trabajo, que permite añadir un espacio de trabajo Eclipse o IBM Rational Application Developer for WebSphere Software (RAD) existente que contiene proyectos Java. Una vez importado el espacio de trabajo, podrá escanear los proyectos Java que contiene.
- Nota:** Antes de importar un espacio de trabajo, asegúrese de haber instalado y actualizado el entorno de desarrollo tal como se describe en “Configuración del entorno de desarrollo para proyectos de Eclipse y Rational Application Developer for WebSphere Software (RAD)” en la página 47.
- **Descubrir aplicaciones:** Esto inicia Application Discovery Assistant, que permite crear y configurar aplicaciones y proyectos con rapidez para código fuente Java y Microsoft Visual Studio
- **Expandir todo**
- **Contraer todo**
- **Propiedades:** al seleccionarla, se abre la vista Propiedades para el elemento seleccionado.
- Al seleccionar una aplicación en la sección Explorador, estas opciones del menú que aparece al pulsar el botón derecho del ratón están disponibles:
  - **Escanear la aplicación:** Escanear la aplicación proyecto o archivo seleccionados. El escaneo se ejecutará con la configuración de escaneo predeterminada.
  - **Escanear aplicación con:** Seleccione la configuración de escaneo que desee utilizar. O bien, seleccione la acción **Editar configuraciones** para establecer una configuración de escaneo diferente como valor predeterminado (en la vista Configuración del escaneo, seleccione la configuración que desea establecer como valor predeterminado y, a continuación, pulse **Seleccionar como valor predeterminado**).



- **Añadir proyecto**
  - **Nuevo proyecto:** Si una aplicación está en la vista Explorador, esta acción está disponible y al seleccionarla le permite añadir un nuevo proyecto a la aplicación. Esta acción inicia el Asistente de proyecto nuevo.
  - **Proyecto existente:** Si una aplicación está en la vista Explorador, esta acción está disponible y al seleccionarla le permite añadir un proyecto existente en la aplicación. Esta acción inicia un cuadro de diálogo que permite buscar archivos .ppf, .vcproj, .vcxproj, .csproj, .vbproj, .dsp, o .epf para abrirlos.
  - **Varios proyectos:** Añadir varios proyectos a la aplicación que está seleccionada en la vista Explorador. Esta acción muestra un recuadro de diálogo que le permite completar una de estas tareas:
    - Especificar un directorio en el que buscar proyectos.
    - Especificar un espacio de trabajo en el que buscar proyectos.
    - Especificar un archivo Microsoft Solution en el que buscar proyectos.
 En estos resultados, puede seleccionar una o varios proyectos que añadir.
- **Eliminar aplicación:** Si una aplicación está en la vista Explorador, esta acción está disponible y al seleccionarla se eliminan las aplicaciones seleccionadas.
- **Añadir resultado personalizado:** esta acción inicia el cuadro de diálogo Crear resultado personalizado, que le permite crear un resultado personalizado para la aplicación seleccionada.
- **Renovar:** Renuevo el contenido de la aplicación, proyecto o vista seleccionada.
- Registrar/eliminar registro:
  - **Registrar aplicación:** Registrar la aplicación o proyecto seleccionado con AppScan Source. Debe registrar aplicaciones y proyectos primero para que se puedan publicar en la base de datos de AppScan Source.
  - **Registrar aplicación como...:** seleccione esta opción para registrar una aplicación con un nuevo nombre.
  - **Eliminar registro de la aplicación:** Anular el registro de la aplicación o proyecto seleccionado.
  - **Localizar:** seleccione esta opción para asociar una aplicación o proyecto local con uno que haya registrado otro usuario de AppScan Source.
- **Expandir todo**
- **Contraer todo**
- **Propiedades:** al seleccionarla, se abre la vista Propiedades para el elemento seleccionado.
- Al seleccionar un proyecto en la sección Explorador, estas opciones del menú que aparece al pulsar el botón derecho del ratón están disponibles:
  - **Escanear proyecto:** Escanear la aplicación proyecto o archivo seleccionados. El escaneo se ejecutará con la configuración de escaneo predeterminada.
  - **Escanear proyecto con:** Seleccione la configuración de escaneo que desee utilizar. O bien, seleccione la acción **Editar configuraciones** para establecer una configuración de escaneo diferente como valor predeterminado (en la vista Configuración del escaneo, seleccione la configuración que desea establecer como valor predeterminado y, a continuación, pulse **Seleccionar como valor predeterminado**).
  - **Copiar proyecto:** Si se selecciona un proyecto en la vista Explorador, esta acción está disponible y al seleccionarla abre un cuadro de diálogo que le

permite copiar el proyecto a otra aplicación o crear una copia del proyecto en la aplicación que actualmente contenga el proyecto.

- **Eliminar proyecto:** Eliminar el objeto seleccionado.
- Registrar/eliminar registro:
  - **Registrar proyecto:** Registrar la aplicación o proyecto seleccionado con AppScan Source. Debe registrar aplicaciones y proyectos primero para que se puedan publicar en la base de datos de AppScan Source.
  - **Eliminar registro del proyecto:** Anular el registro de la aplicación o proyecto seleccionado.
  - **Localizar:** seleccione esta opción para asociar una aplicación o proyecto local con uno que haya registrado otro usuario de AppScan Source.
- **Expandir todo**
- **Contraer todo**
- **Propiedades:** al seleccionarla, se abre la vista Propiedades para el elemento seleccionado.
- Al seleccionar un archivo en la sección Explorador, estas opciones del menú que aparece al pulsar el botón derecho del ratón están disponibles:
  - **Escanear archivo:** Escanear la aplicación proyecto o archivo seleccionados. El escaneo se ejecutará con la configuración de escaneo predeterminada.
  - **Escanear archivo con:** Seleccione la configuración de escaneo que desee utilizar. O bien, seleccione la acción **Editar configuraciones** para establecer una configuración de escaneo diferente como valor predeterminado (en la vista Configuración del escaneo, seleccione la configuración que desea establecer como valor predeterminado y, a continuación, pulse **Seleccionar como valor predeterminado**).
  - **Excluir de los escaneos:** elimina de los escaneos el archivo seleccionado.
  - **Abrir en editor interno:** abre el archivo seleccionado en el editor de AppScan Source (en la perspectiva Análisis).
  - **Abrir en editor externo:** escoja un editor externo en el que abrir el archivo seleccionado.
  - **Propiedades:** al seleccionarla, se abre la vista Propiedades para el elemento seleccionado.

## Indicadores de aplicaciones y proyectos

Esta tabla identifica los iconos de aplicación y de proyecto de la vista Explorador.

*Tabla 9. Iconos de aplicación y de proyecto*

| Tipo de aplicación o proyecto                                                     | No registrado                                                                       | Registrado                                                                          | Falta/No se encuentra                                                                 |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| Aplicación importada                                                              |  |  |  |
| Aplicación creada manualmente o creada utilizando Application Discovery Assistant |  |  |  |
| Proyecto importado                                                                |  |  |  |

Tabla 9. Iconos de aplicación y de proyecto (continuación)

| Tipo de aplicación o proyecto                                                   | No registrado                                                                     | Registrado                                                                        | Falta/No se encuentra                                                               |
|---------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Proyecto creado manualmente o creada utilizando Application Discovery Assistant |  |  |  |

La vista Explorador muestra aplicaciones y proyectos locales, así como aquellos registrados en el servidor (los registrados en el servidor que no se han guardado localmente, por ejemplo, las aplicaciones y los proyectos registrados por otros usuarios, aparecen sombreados). Si pulsa el botón **Menú Ver** de la barra de herramientas y conmuta al elemento de menú **Ocultar elementos registrados en el servidor** para que no esté seleccionado, puede ver las aplicaciones y proyectos del servidor existentes. Si un proyecto aparece sombreado, puede pulsar con el botón derecho y seleccionar **Localizar** en el menú.



---

## Capítulo 3. Preferencias

Las preferencias son seleccione personales sobre el aspecto y el funcionamiento de AppScan Source for Analysis.

Para abrir las páginas de preferencias, seleccione **Editar > Preferencias** en el menú principal del entorno de trabajo. Puede examinar las preferencias consultando todos los títulos del panel izquierdo o puede buscar un grupo más reducido de títulos utilizando el campo de filtro que hay en la parte superior del panel izquierdo. Los resultados que devuelve el filtro coinciden con los títulos de las páginas de preferencias y con palabras clave como JSP o correo electrónico.

Los controles de flecha de la parte superior derecha del panel derecho le permiten ir a páginas vistas anteriormente. Para volver a una página después de ver varias páginas, pulse en la flecha hacia abajo para ver una lista de las páginas de preferencias vistas recientemente.

---

### Preferencias generales

Las preferencias generales le permiten personalizar algunos de los valores predeterminados de AppScan Source for Analysis para adaptarlos a sus preferencias personales.

#### Seleccionar un idioma

La interfaz de usuario de AppScan Source for Analysis se puede visualizar en varios idiomas. Para cambiar el idioma mostrado, selecciónelo en la lista **Seleccionar un idioma** y pulse **Aceptar** en el cuadro de diálogo de preferencias. Debe reiniciar manualmente el espacio de trabajo para que los cambios entren en vigor.

**Nota:** Para utilizar esta característica, se debe instalar al menos un paquete de idioma durante el procedimiento de instalación. Si el único idioma instalado es el inglés, el producto se visualizará en inglés tras usar esta preferencia y reiniciar el espacio de trabajo. En este caso, si desea visualizar la interfaz de usuario en otro idioma, vuelva a ejecutar el asistente de instalación y elija reparar la instalación añadiendo uno o varios paquetes de idioma.

#### Codificación del archivo

La codificación de caracteres de los archivos del proyecto debe establecerse de modo que AppScan Source pueda leer los archivos correctamente (y, por ejemplo, mostrarlos correctamente en la vista de origen). Seleccione la codificación de caracteres predeterminada en esta sección.

#### Nivel de registro

Puede modificar el nivel de registro para obtener el nivel de información que desee en los registros de errores. Elija entre **Rastreo**, **Depuración**, **Información**, **Avisos**, **Errores** y **Muy grave**, donde **Rastreo** ofrece el nivel más ruidoso de registro, **Muy grave** registra solo los sucesos críticos y los valores restantes, para ofrecer niveles cada vez más altos de registro.

## **Guardar todos los filtros al salir**

Si esta opción está seleccionada, se inhabilita un indicador para guardar automáticamente todos los filtros recién creados o editados al salir de AppScan Source.

## **Cancelar escaneo cuando se produzca un error**

Si está seleccionada, se impiden los escaneos incompletos cancelando un escaneo si se produce un error.

## **Crear un marcador para cada resultado**

Cuando está seleccionada esta opción, y si tiene un asesoramiento abierto, el origen del escaneo abierto en el editor incluirá marcadores a ubicaciones para las que hay resultados.

De forma predeterminada, la creación de marcadores está habilitada.

La creación de marcadores puede ralentizar un escaneo. Si el proyecto incluye muchos archivos de origen (o archivos de origen de gran tamaño), se puede mejorar el rendimiento desactivando la creación de marcadores.

## **Después de que finalice un escaneo**

El valor predeterminado consiste en recibir un indicador que le pregunta si desea que el asesoramiento se abra automáticamente al final de un escaneo. Si no desea ver el indicador, seleccione **Abrir siempre el asesoramiento nuevo** o **No abrir nunca**.

## **Después de que se complete un escaneo y existan escaneos no guardados de los mismos destinos**

De forma predeterminada, se le pedirá que guarde o descarte los escaneos no guardados existentes. Puede modificar esta preferencia de modo que los escaneos duplicados se supriman automáticamente siempre o no se supriman nunca automáticamente. Cuando se establece esta preferencia, tenga en cuenta que el uso de la memoria se reduce cuando los escaneos duplicados se suprimen.

## **Al publicar o exportar un asesoramiento con vías de acceso absolutas**

De forma predeterminada, se le solicitará que defina variables de vía de acceso absolutas cuando publique. Los valores de esta sección le permiten inhabilitar esta solicitud predeterminada o abrir automáticamente el recuadro de diálogo que le permite definir variables cuando existan vías de acceso absolutas.

## **Aplicaciones registradas automáticamente en una publicación inicial**

De forma predeterminada, cuando publique asesoramientos para aplicaciones o proyectos que no están registrados, se le solicitará que los registre. Puede elegir registrar siempre aplicaciones y proyectos cuando se publiquen o no registrarlos nunca.

**Importante:** Debe tener permiso **Registrar** para poder registrar aplicaciones y proyectos.

## Cuando hay conflictos de nombres de aplicación

Es posible tener aplicaciones del mismo nombre en AppScan Source for Analysis, sin embargo, trabajar con ellos puede no ser manejable. De forma predeterminada, si intenta dar una aplicación con el mismo nombre que una aplicación existente (o importar una aplicación con el mismo nombre que una aplicación existente), recibirá una solicitud de aviso. El mensaje de aviso le permite generar un nombre exclusivo para la aplicación, conservar el nombre en conflicto o cancelar la operación.

Si desea que AppScan Source for Analysis genere automáticamente un nombre de aplicación exclusivo cuando surgen conflictos, seleccione **Generar un nombre exclusivo** en la página de preferencias. Si desea aceptar automáticamente los nombres de aplicación en conflicto, seleccione **Mantener el nombre existente**.

**Nota:** Las aplicaciones se almacenan con el nombre de archivo <nombre\_aplicación>.paf. Si selecciona **Mantener el nombre existente**, puede establecer el directorio de trabajo para que sea el mismo que el de la aplicación existente con el mismo nombre. En este caso, se le solicitará si desea sobrescribir el nombre de archivo existente, pero la sobrescritura fallará porque la aplicación existente ya está abierta en AppScan Source for Analysis.

## Cuando hay conflictos de nombres de proyecto

Este valor sólo se aplica cuando se intenta crear o importar un proyecto con el mismo nombre que uno que ya existe en la misma aplicación. En este caso, los nombres de proyecto no puede entrar en conflicto. Si lo intenta, de forma predeterminada, se le solicitará que tenga un nombre exclusivo generado o que cancele la acción. Si desea que AppScan Source for Analysis genere automáticamente un nombre de proyecto exclusivo cuando surgen conflictos, seleccione **Generar un nombre exclusivo** en la página de preferencias.

## Número de asesoramientos que se mostraron en Asesoramientos publicados y Mis asesoramientos al inicio

Establezca el número máximo de asesoramientos que desea ver en la vista Asesoramientos publicados o Mis asesoramientos.

## Canal de información RSS que se visualiza en la vista de bienvenida

De forma predeterminada, la vista de bienvenida muestra contenido de canal de información RSS de X-Force. Para mostrar otro contenido, especifique el URL que desee en el campo **Canal de información RSS que se visualiza en la vista de bienvenida**.

## Optimizar High Network Latency

Seleccione este recuadro de selección para almacenar en la memoria caché más información sobre el cliente de modo que se minimicen las llamadas del servidor.

## Volver a cargar la configuración del sistema

Cargar los últimos valores del sistema. Si ha cambiado los valores fuera del producto, mientras este se está ejecutando, por ejemplo, modificando los archivos .ozsettings en <data\_dir>\config (donde <data\_dir> es la ubicación de los datos de programa AppScan Source, como se describe en “Instalación y ubicaciones de archivo de datos de usuario” en la página 335) - seleccione este botón para renovar los valores en el producto.

---

## Preferencias de AppScan Enterprise Console

Si AppScan Enterprise Server se ha instalado con la opción AppScan Enterprise Console, puede publicar asesoramientos en la misma. Enterprise Console ofrece una variedad de herramientas para trabajar con asesoramientos, como característica de informes, gestión de problemas, análisis de tendencias y paneles de control.

Para habilitar esta función, complete la página de preferencias de AppScan Enterprise Console. Todos los campos de esta página deben completarse con entradas válidas para que se habilite la publicación de Enterprise Console:

- **Campo ID de usuario:** Especifique su ID de usuario de AppScan Enterprise Server (el ID de usuario que se creó para la publicación en representación de su usuario de AppScan Source).
  - Si se ha configurado AppScan Enterprise Server para utilizar la autenticación de Windows, escriba el dominio y el nombre de usuario que utiliza para conectarse con Enterprise Console (separe el dominio y el nombre de usuario con una barra invertida, \, por ejemplo, mi\_dominio\mi\_nombreusuario).
  - Si se ha configurado AppScan Enterprise Server con LDAP, escriba el nombre de usuario que ha utilizado para conectarse con Enterprise Console.
  - En Windows, si AppScan Enterprise Server está habilitado para la autenticación CAC (Common Access Card), seleccione su Nombre común CAC de la lista.

Como mínimo, debe ser un usuario de QuickScan. Si está conectado a una instancia de AppScan Enterprise Server anterior a la versión 9.0.3, debe tener su propia carpeta en Enterprise Server.

- **Campo Contraseña:** Este campo únicamente está disponible si su método de autenticación de AppScan Enterprise Server es mediante ID de usuario y contraseña. Especifique la contraseña que se ha utilizado para iniciar sesión en Enterprise Console (la contraseña para el nombre de usuario que se ha entrado).
- **Campo URL de Enterprise Console:** Especifique el URL utilizado para acceder a la aplicación web de Enterprise Console.

El formato de esta URL es:

http(s)://<nombrehost>:<puerto>/ase

Donde <nombrehost> es el nombre de la máquina en la que se ha instalado Enterprise Console y <puerto> es el puerto en el que la consola está en ejecución (el <puerto> predeterminado es 9443). Un ejemplo de URL es <https://myhost.mydomain.ibm.com:9443/ase>.

### Nota:

- Este campo no se ha de modificar si ya se ha definido **URL de Enterprise Console**.
- Debe haber iniciado la sesión en AppScan Source con permiso para **Gestionar configuraciones de AppScan Enterprise** para poder definir el campo **URL de Enterprise Console**. Para obtener información sobre cuentas y permisos de



usuarios, consulte la sección sobre *Administración* del InfoCenter del producto o la sección *Administración de AppScan Source* de la publicación *IBM Security AppScan Source Guía de instalación y administración*.

- El **ID de usuario** y la **Contraseña** se guardan en la máquina que ejecuta el cliente de AppScan Source (por ejemplo, AppScan Source for Analysis) - mientras que **URL de Enterprise Console** se guarda en Enterprise Server (que puede estar ubicado en una máquina remota). No puede acceder a la información del nombre de usuario y contraseña desde la máquina remota (por ejemplo, utilizando el mandato `getaseinfo` desde la misma).
- AppScan Source no da soporte a la publicación en una instancia de AppScan Enterprise Console que se haya configurado para utilizar valores de proxy. Si se intenta publicar en una instancia que utiliza valores de proxy, se producirá un error.

Tras completar los valores, se recomienda encarecidamente asegurarse de que la conexión con el servidor de Enterprise Console sea válida pulsando **Probar conexión**.

**Consejo:** Si la prueba de conexión falla, compruebe que el servidor de Enterprise Console se esté ejecutando y que pueda acceder a su URL de centro de control en un navegador (utilice el mismo valor de **URL de Enterprise Console** que ha especificado anteriormente).

---

## Preferencias del servidor de aplicaciones para la compilación de JavaServer Page

Si está escaneando una aplicación que contiene JavaServer Pages (JSP), el motor de análisis de AppScan Source debe ser capaz de compilar el código JSP para poderlo analizar. Cuando cree el proyecto JSP, debe especificar el compilador JSP que debe utilizar AppScan Source (o aceptar el compilador predeterminado, que se puede establecer en la página de preferencias de Java y JSP). Si AppScan Source no puede compilar los archivos JSP, utilice las páginas de preferencias del servidor de aplicaciones para configurar el compilador JSP que utiliza la aplicación.

La instalación de AppScan Source incluye Apache Tomcat Versiones 7 y 8. Si las páginas de preferencias de **Tomcat 7** y **Tomcat 8** no están configuradas, AppScan Source compilará los archivos JSP mediante el compilador Tomcat JSP proporcionado que actualmente está marcado como predeterminado. Si desea utilizar un compilador Tomcat soportado externo, utilice la página de preferencias de Tomcat para apuntar a la instalación local de Tomcat.

Si utiliza Oracle WebLogic Server o WebSphere Application Server, debe configurar la página de preferencias correspondiente para que apunte a la instalación local del servidor de aplicaciones a fin de que se pueda utilizar para la compilación de JSP durante el análisis (si crea un proyecto JSP sin configurar primero el servidor de aplicaciones, se solicitará que lo configure en dicho momento).

### Tomcat

En este tema se describen las preferencias que debe establecer para configurar AppScan Source de modo que haga referencia a un servidor de aplicaciones Apache Tomcat, que no sea el que se proporciona con AppScan Source.

La instalación de AppScan Source incluye Apache Tomcat Versiones 7 y 8. Si las páginas de preferencias de **Tomcat 7** y **Tomcat 8** no están configuradas, AppScan

Source compilará los archivos JSP mediante el compilador Tomcat JSP proporcionado que actualmente está marcado como predeterminado. Si desea utilizar un compilador Tomcat soportado externo, utilice la página de preferencias de Tomcat para apuntar a la instalación local de Tomcat.

Si utiliza un compilador Tomcat externo soportado, vaya a la página de preferencias adecuada y defina el directorio de instalación del servidor de aplicaciones. Si especifica el directorio de instalación, AppScan Source podrá encontrar automáticamente todas las dependencias del servidor de aplicaciones cuando configure proyectos.

## WebLogic 11 y 12

En este tema se describen las preferencias que debe establecer para configurar AppScan Source de modo que haga referencia a Oracle WebLogic Server.

En las páginas de preferencias de WebLogic, especifique el directorio de instalación del servidor; también puede establecer opciones de configuración avanzadas. Si especifica el directorio de instalación, AppScan Source podrá encontrar automáticamente todas las dependencias del servidor de aplicaciones cuando configure proyectos.

Configure AppScan Source de modo que haga referencia al directorio de instalación de WebLogic, al archivo JAR de WebLogic y a las opciones del compilador JavaServer Page (JSP).

Solo marque el cuadro de selección **Habilitar opciones de configuración avanzadas** si necesita cambiar las opciones del compilador WebLogic JSP o localizar el archivo `weblogic.jar`. El valor predeterminado de opciones del compilador WebLogic JSP es:

```
%JSP_JVM_OPTIONS%  
-Dcom.sun.xml.namespace.QName.useCompatibleSerialVersionUID=1.0  
-classpath  
%JSP_COMPILER_CLASSPATH% weblogic.jspc  
%JSP_OPTIONS% -verboseJspc -package  
%PACKAGE_NAME% -linenumbers -g -debug -keepgenerated -compiler  
%JAVAC_PATH% -webapp  
%WEB_CONTEXT_ROOT_PATH% -d  
%OUTPUT_PATH%
```

## WebSphere Application Server

En este tema se describen las preferencias que debe establecer para configurar AppScan Source de modo que haga referencia a WebSphere Application Server para la compilación de JSP.

Para conocer a qué versiones de WebSphere Application Server da soporte AppScan Source, consulte <http://www.ibm.com/support/docview.wss?uid=swg27027486>.

En las páginas de preferencias de WebSphere Application Server, especifique el directorio de instalación del servidor; también puede establecer opciones de configuración avanzadas. Si especifica el directorio de instalación, AppScan Source podrá encontrar y utilizar el compilador JSP de WebSphere Application Server.

Configure AppScan Source para que haga referencia al directorio de instalación de WebSphere Application Server. Además, las opciones de configuración avanzadas le

permiten establecer la línea de mandatos del compilador JSP de WebSphere Application Server y la vía de acceso de clase (classpath).

Únicamente seleccione el recuadro de selección **Habilitar opciones de configuración avanzadas** para WebSphere Application Server personalizar la línea de mandatos JSP de WebSphere Application Server o para especificar una vía de acceso a clases distinta de la vía de acceso a clases de WebSphere Application Server (modifique este valor si desea incluir archivos jar adicionales en la vía de acceso a clases que todas sus aplicaciones de WebSphere Application Server utilizarán).

La opción de línea de mandatos del compilador JSP de WebSphere Application Server predeterminada es:

```
%CMD_EXE% %CMD_ARGS%  
'%FILE(%%JSP_COMPILER_INSTALL_DIR%/bin/JspBatchCompiler%BAT%%)%'  
-response.file  
'%TMP_FILE(%-keepgenerated=true -recurse=true -useFullPackageNames=true  
-verbose=false -createDebugClassfiles=true -jsp.file.extensions=%WEB_EXTS%  
-javaEncoding=%ENCODING%  
%JSP_OPTIONS% %QUOTE%-war.path=%WEB_CONTEXT_ROOT_PATH%QUOTE%  
%QUOTE%-filename=%RELATIVE_FILENAME_NO_QUOTE% %QUOTE% %)'
```

---

## Definición de variables

Cuando guarda asesoramientos o paquetes, o cuando publica asesoramientos, es posible que AppScan Source for Analysis le sugiera que cree una variable para sustituir las vías de acceso absolutas (sin variables, AppScan Source for Analysis graba las vías de acceso absolutas en el archivo de asesoramiento para hacer referencia a elementos, tales como los archivos de origen). Cuando configura variables para vías de acceso absolutas, facilita que se compartan los asesoramientos en varios sistemas. Cuando se comparten asesoramientos, se recomienda utilizar variables.

### Acerca de esta tarea

Las variables se pueden crear antes de iniciar una acción de guardar o publicar siguiendo las instrucciones de este tema, o bien se pueden crear después de iniciar la acción de guardar o publicar siguiendo los pasos del tema “Definición de variables cuando se publican y se guardan” en la página 142.

Por ejemplo, para obtener información acerca de cómo las variables pueden servir de ayuda cuando se comparten asesoramientos, consulte la sección “Ejemplo: definición de variables” en la página 142.

### Procedimiento

1. En el menú principal, seleccione **Ventana > Preferencias**. En el cuadro de diálogo Preferencias, seleccione **Cambiar variables**.
2. Pulse el botón **Añadir variable** en la página de preferencias Cambiar variables.
3. Entre un nombre para la variable y vaya a la ubicación del archivo, que será sustituido por la variable (AppScan Source for Analysis inserta los símbolos de porcentaje (%) al inicio y fin después de que se crea la variable).
4. Repita el paso anterior para cualquier otro elemento de referencia del asesoramiento (por ejemplo, si el asesoramiento hace referencia al origen en varias ubicaciones, añada una variable para cada ubicación).
5. Utilice la página de preferencias para editar y eliminar variables, mediante los botones **Modificar variable** y **Suprimir variable**.

6. Pulse **Aceptar** cuando haya acabado de definir las variables.

---

## Habilitación del seguimiento de defectos con preferencias

Las preferencias del sistema de seguimiento de defectos le permiten habilitar el envío de resultados a un sistema de seguimiento de defectos y determinar cómo se envían defectos.

El separador General de la página de preferencias del sistema de seguimiento de defectos sirve para habilitar o inhabilitar la característica de integración Sistema de seguimiento de defectos en AppScan Source. Si el cuadro de selección **Habilitar integración Defect Tracking System** está marcado, la acción del menú de contexto **Enviar defecto** estará disponible para los resultados de asesoramiento. El separador General también permite realizar cierto control sobre los sistemas de seguimiento de defectos que estarán disponibles cuando se envíen defectos.

Para obtener más información sobre las preferencias que se pueden definir para los sistemas de seguimiento de defectos soportados, consulte estos temas de ayuda:

- “Preferencias de Rational ClearQuest”
- “Preferencias de Quality Center” en la página 101
- “Preferencias de Rational Team Concert” en la página 103
- “Preferencias de Team Foundation Server” en la página 104

### Preferencias de Rational ClearQuest

Para poder completar las preferencias de Rational ClearQuest, el administrador de Rational ClearQuest deberá proporcionarle los valores de Rational ClearQuest necesarios. Los valores son específicos del entorno de Rational ClearQuest.

**Nota:** Cuando se integra con Rational ClearQuest versión 8.0, el esquema Rational ClearQuest debe contener los campos disponibles en el esquema **DefectTracking** predefinido.

### Conjunto de base de datos

Una colección de una o varias bases de datos de defectos.

Valor predeterminado de Linux = Nombre de conexión,  
Nombre predeterminado de Windows = Conjunto de base de datos

### Nombre de base de datos

Nombre de la base de datos a la que se enviarán los defectos.

### Nombre de usuario de base de datos

Nombre de usuario de base de datos de Rational ClearQuest predeterminado.

### Ubicación de CQPerl ejecutable

Ubicación del archivo ejecutable de CQPerl de Rational ClearQuest en el sistema local. La ubicación predeterminada especificada se correlaciona con la ubicación de instalación de Rational ClearQuest predeterminada.

## **Entidad para registros defectuosos**

Entidad (objeto de base de datos) configurada por la instalación de Rational ClearQuest que se utilizará para objetos defectuosos.

La entidad predeterminada es **Defecto**.

## **Campo descripción en el registro**

La descripción predeterminada es **Descripción**.

## **Campo encabezamiento en el registro**

El encabezamiento predeterminado es **Encabezamiento**.

## **Defecto único por cada resultado**

Enviar un grupo de resultados como un único defecto o como varios defectos. Puede cambiar el método de envío cuando cree el defecto.

## **Preferencias de Quality Center**

Primero debe habilitar HP Quality Center como una preferencia general del sistema de seguimiento de defectos y luego debe establecer la preferencia individual en el separador Quality Center.

### **URL del servidor**

El URL del servidor de Quality Center, por ejemplo, `http://<hostname>:<port>/qcbin/` o `https://<hostname>:<port>/qcbin/`.

### **Nombre de usuario (opcional)**

Un nombre de usuario para iniciar una sesión en Quality Center

### **Contraseña (opcional)**

Si ha especificado un nombre de usuario, especifique la contraseña correspondiente

### **Dominio**

El dominio de Quality Center con el que va a establecer conexión.

### **Proyecto**

El proyecto de Quality Center con el que va a establecer conexión

### **Iniciar sesión automáticamente**

Cuando esta opción está habilitada, AppScan Source no solicita información de inicio de sesión al enviar resultados e inicia la sesión con las credenciales predeterminadas especificadas en las Preferencias. Si no está habilitada, debe iniciar la sesión cada vez que envíe un resultado a Quality Center.

## Enviar automáticamente

Cuando esta opción está habilitada, el cuadro de diálogo utilizado para enviar nuevos defectos no aparece cuando se envían resultados. AppScan Source for Analysis utiliza las **Propiedades de defecto predeterminadas** especificadas en las Preferencias. Si no está habilitada, se le solicita que especifique información sobre el defecto (Gravedad, Prioridad, Tipo de defecto, Estado, etc.) cuando envía resultados.

## Reenvío de resultados enviados previamente

Los resultados enviados a Quality Center se etiquetan con información sobre el defecto (ID de defecto, usuario remitente y fecha del envío). De forma predeterminada, AppScan Source no reenvía el mismo resultado más de una vez. Esto le permite asignar varios resultados a Quality Center, especificando únicamente los nuevos resultados en la base de datos de Quality Center. Cuando esta opción está seleccionada (verdadera), los resultados enviados previamente se pueden reenviar a Quality Center.

## Envío de cada resultado como un error individual

Cuando se envían varios resultados en una sola operación, puede enviar todos los resultados como un solo defecto de Quality Center o como un defecto de Quality Center separado para cada resultado individual de AppScan Source. Si se marca este cuadro de selección, la etiqueta se establece en verdadera, creando un defecto separado de Quality Center para cada resultado individual. Si se establece la etiqueta en falsa, se crea un defecto de Quality Center para todos los resultados enviados como parte de un envío masivo.

## Generar automáticamente resumen de errores

Cuando es verdadero, AppScan Source genera automáticamente un resumen de defectos para el envío a Quality Center. El resumen indica el número de resultados incluidos y el defecto y el tipo de resultados incluidos, como por ejemplo `Validation.Required`.

Cuando es falso, aparece el campo Resumen para que el usuario lo complete cuando envíe el defecto en el cuadro de diálogo que se abre al abrir un nuevo defecto.

## Carga automática de campos de errores

El valor predeterminado es verdadero. Cuando este cuadro de selección está marcado, AppScan Source carga automáticamente definiciones de campos de defectos de la base de datos de Quality Center, en función de los valores actuales de usuario y de grupo en Quality Center. Cuando es falso, AppScan Source no muestra campos de defectos de Quality Center en el cuadro de diálogo que se abre al abrir un nuevo defecto.

## Propiedades de defecto predeterminadas

Para establecer valores predeterminados para distintos atributos de defecto de Quality Center, pulse **Propiedades de defecto predeterminadas** en el separador de preferencias de Quality Center. Los valores predeterminados se incluyen en el

cuadro de diálogo **Nuevo defecto** en el momento del envío o se envían silenciosamente a Quality Center si la preferencia **Enviar automáticamente** está seleccionada.

**Nota:** Las propiedades de defectos y sus valores disponibles se obtienen de forma dinámica de Quality Center cada vez que aparece el cuadro de diálogo **Propiedades de defecto** si **Cargar automáticamente campos de errores** está seleccionado. Por lo tanto, los nuevos campos y valores añadidos a la base de datos de Quality Center aparecen automáticamente en AppScan Source for Analysis. Se necesita información válida sobre servidor, inicio de sesión y conexión para abrir y llenar el cuadro de diálogo **Propiedades de defecto** con información de Quality Center.

### Personalización de campos de defectos de Quality Center

A través de un archivo de configuración, puede personalizar los campos y las interacciones entre dichos campos en el cuadro de diálogo **Nuevo defecto**. Encontrará un archivo de configuración de ejemplo en `<data_dir>\config\qc.dts` (donde `<data_dir>` es la ubicación de los datos de programa AppScan Source, como se describe en “Instalación y ubicaciones de archivo de datos de usuario” en la página 335), que contiene personalizaciones de ejemplo y documentación adicional. Estas personalizaciones le permiten modelar la lógica del script de flujo de trabajo de Quality Center directamente en el cuadro de diálogo **Nuevo defecto**.

Las personalizaciones disponibles incluyen:

- Visualizar campos personalizados, campos que faltan o ambos
- Imponer que algunos campos siempre se visualicen (modificando los valores de Quality Center)
- Actualizar el estado necesario de los campos en función de la selección de otros campos
- Actualizar dinámicamente opciones de cuadro de lista para un campo en función de la selección del cuadro de lista de otro campo

## Preferencias de Rational Team Concert

El separador Preferencias de Rational Team Concert le permite configurar una conexión con el servidor de Rational Team Concert y configurar los valores de los atributos de los elementos de trabajo.

Cuando haya especificado información sobre la conexión y haya iniciado correctamente la sesión, podrá conectar con una o varias áreas de proyecto. Cada área de proyecto puede tener su propia configuración de valores preestablecidos de atributos.

**Nota:** Al conectarse a Rational Team Concert (configurando preferencias o enviando defectos), puede que se le solicite que acepte un certificado SSL. Consulte el apartado “Certificados SSL de Rational Team Concert” en la página 104 para obtener más información.

Para configurar los valores de atributos para una determinada área de proyecto, seleccione el área de proyecto y elija **Configurar**. En el cuadro de diálogo de configuración, puede especificar valores de atributos como valores codificados y, en algunos casos, como variables que hagan referencia a un resultado seleccionado. Por ejemplo, si se usa `{Finding.fileName}` en un valor de atributo, se sustituirá por el nombre de archivo real del código fuente correspondiente a un resultado durante el envío. Dispone de asistencia de contenido (`<Control>+<Espacio>`) para los valores de atributos que dan soporte a estas variables. Se recomienda a los

equipos que compartan estas configuraciones utilizando los botones **Importar** y **Exportar** disponibles en la página de preferencias principal de Rational Team Concert.

## **Certificados SSL de Rational Team Concert**

Cuando se instala el servidor Rational Team Concert, se debe configurar de modo que utilice un certificado SSL válido. Si no se hace, recibirá un mensaje de conexión no fiable cuando inicie la sesión en el servidor (configurando preferencias o enviando defectos). Este tema muestra las consideraciones del certificado SSL de Rational Team Concert.

## **Ubicación del almacenamiento de certificados SSL**

Los certificados que se han aceptado de forma permanente se guardan en `<user_home>/jazzcerts` (donde `<user_home>` es el directorio de inicio del sistema operativo (por ejemplo, en Windows, el directorio puede ser `C:\Documents and Settings\Administrator\`)). Al eliminar `<user_home>/jazzcerts` se eliminan todos los certificados almacenados para los clientes de AppScan Source y Rational Team Concert.

## **El certificado SSL se comparte con los clientes Rational Team Concert**

AppScan Source comparte su almacén de certificados con clientes de Rational Team Concert. Si acepta de forma definitiva un certificado utilizando un cliente de Rational Team Concert, AppScan Source lo reutilizará (no se le solicitará en AppScan Source que acepte un certificado). De manera similar, si acepta de forma definitiva un certificado en AppScan Source, los clientes de Rational Team Concert lo reutilizarán.

## **Consideraciones de red denominación de servidores de Rational Team Concert cuando se realiza el seguimiento de defectos desde AppScan Source for Analysis**

Si ha habilitado el seguimiento de defectos de Rational Team Concert en AppScan Source for Analysis, y se modifica el nombre del servidor de Rational Team Concert, la configuración existente de las áreas de proyecto en ese servidor ya no estarán disponibles en AppScan Source for Analysis. Deberá conectarse al servidor a través de su URI de repositorio y volver a crear la configuración en las preferencias del sistema de seguimiento de defectos.

## **Preferencias de Team Foundation Server**

El separador Preferencias de Team Foundation Server permite configurar una conexión con un Microsoft Team Foundation Server y configurar los valores de los campos de elementos de trabajo.

Cuando haya especificado información sobre la conexión y haya iniciado correctamente la sesión, podrá conectar con uno o varios proyectos.

**Nota:** Al configurar el inicio de sesión para Team Foundation Server 2010, el URL del servidor debe contener la Recopilación de proyecto de equipo a la que se desea conectar. Por ejemplo, `http://myserver:8080/tfs/Recopilación_predeterminada`.

Cada proyecto puede tener su propia configuración de valores preestablecidos de campos.

Para configurar los valores de campos para un determinado proyecto, seleccione el proyecto y elija **Configurar**. En el cuadro de diálogo de configuración, puede



especificar valores de campos como valores codificados y, en algunos casos, como variables que hagan referencia a un resultado seleccionado. Por ejemplo, si se usa {Finding.fileName} en un valor de campo, se sustituirá por el nombre de archivo real del código fuente correspondiente a un resultado durante el envío. Dispone de asistencia de contenido (<Control>+<Espacio>) para los campos que dan soporte a estas variables.

Se recomienda a los equipos que compartan estas configuraciones utilizando los botones **Importar** y **Exportar** disponibles en la página de preferencias principal de Team Foundation Server.

---

## Importadores del espacio de trabajo de Eclipse: configuración de preferencias de Eclipse o Rational Application Developer for WebSphere Software (RAD)

La instalación de AppScan Source for Analysis proporciona un importador predeterminado de Eclipse. Este importador identifica la ubicación de Eclipse y de JRE. Si el importador predeterminado de Eclipse no puede importar su espacio de trabajo, deberá crear un nuevo importador de Eclipse.

### Antes de empezar

Cada configuración de importador representa una instalación de Eclipse o Rational Application Developer for WebSphere Software (RAD). Para utilizar estas configuraciones para importar los espacios de trabajo y proyectos existentes a AppScan Source for Analysis, deberá instalar también los plug-ins de AppScan Source for Development en el entorno de Eclipse.

Antes de añadir un espacio de trabajo de RAD, debe crear una configuración para el tipo de espacio de trabajo.

### Procedimiento

1. En AppScan Source for Analysis, seleccione **Editar > Preferencias** en el menú principal del entorno de trabajo.
2. Seleccione **Importadores del espacio de trabajo de Eclipse**.
3. Pulse **Crear una nueva configuración** y, a continuación, complete el cuadro de diálogo Nueva configuración de importación para crear una configuración nueva:

- **Producto:** seleccione el producto adecuado

**Nota:** Si el producto que se ha utilizado para crear el espacio de trabajo no está disponible para su selección, asegúrese de haber completado los pasos de configuración que se describen en “Actualizaciones de Eclipse o Application Developer” en la página 47 antes de intentar crear el importador del espacio de trabajo.

- **Nombre:** nombre del importador
- **Ubicación:** vía de acceso al directorio base de la instalación de Eclipse
- **Ubicación de JRE:** vía de acceso al directorio raíz de Java Runtime Environment (JRE). Utilice un JDK en <install\_dir>\JDKS (donde <dir\_instalación> es la ubicación de la instalación de AppScan Source) o cualquier otro JDK preferido.

4. Pulse en **Aceptar**.

5. Para identificar el importador como valor predeterminado, selecciónelo y pulse **Establecer como predeterminada la configuración seleccionada**. Esto hace que se muestre un icono en la columna **Predeterminado** del importador.

---

## Correo electrónico

Configure los valores de correo electrónico utilizados para enviar resultados bajo la consideración de defectos.

- **A dirección:** dirección de correo electrónico del destinatario. De forma predeterminada, el campo **Enviar a** del recuadro de diálogo Enviar resultados por correo electrónico se llenará con la dirección de correo electrónico. Sin embargo, se puede cambiar fácilmente al preparar el correo electrónico.
- **Dirección remitente:** dirección de correo electrónico del remitente.

**Nota:** Se recomienda una dirección de correo electrónico válida para evitar que el cliente de correo electrónico del destinatario considere el correo electrónico como correo no deseado.

- **Servidor de correo:** servidor de correo de SMTP configurado como mail.myexample.com.

**Importante:** Consulte al administrador del sistema para asegurarse de que tiene la información del servidor de correo electrónico correcta.

---

## Java y JavaServer Pages

Utilice esta página de preferencias para añadir, modificar o suprimir el JDK (Java Development Kit) que se utiliza para escaneos (y para establecer un JDK predeterminado). Asimismo, utilice la página para establecer el compilador JSP (JavaServer Page) predeterminado.

### Predeterminado

Identifica la ubicación del JDK utilizado para escaneos. Un escaneo utiliza el JDK predeterminado cuando el proyecto no especifica un JDK explícitamente. Para establecer el JDK como predeterminado, pulse con el botón derecho sobre el nombre del JDK identificado y a continuación pulse sobre **Establecer JDK predeterminado**. El icono de Predeterminado aparece en la tabla, identificando el JDK predeterminado actual.

**Nota:** El compilador predeterminado, listo para utilizar, para los proyectos JSP es Tomcat 7, y necesita Java Versión 1.6 o superior. Si se mantiene **Tomcat 7** como predeterminado, utilizar un JDK anterior provocará errores de compilación durante los escaneos.

### Nombre y vía de acceso del JDK

Identifica el nombre y ubicación del JDK.

### Compilador predeterminado para proyectos JSP

Tomcat 7, listo para utilizar, es el valor de compilador de JSP predeterminado. Para conocer los compiladores a los que AppScan Source for Analysis da soporte, consulte <http://www.ibm.com/support/docview.wss?uid=swg27027486>.

---

## Artículos de la base de datos de conocimientos

Utilice la página de preferencias Artículos de la base de datos de conocimientos para definir las ubicaciones que contienen artículos de la Base de datos de conocimientos de AppScan Source Security.

La página enumera los directorios que contienen artículos. Para añadir un directorio, pulse **Añadir contenido de directorio** y, a continuación, vaya a la ubicación del artículo. Para eliminar un directorio, selecciónelo y pulse **Eliminar**.

---

## Extensiones de archivo de proyecto

Configure o añada extensiones de archivo global válidas para cada tipo de proyecto, cambie las extensiones para incluir en escaneos, excluya de escaneos y especifique extensiones como archivos web.

Aparece un separador de página para cada tipo de proyecto o lenguaje: Java, JavaScript, ASP, Perl, PHP, ColdFusion, PBSA (para tipos de proyecto basados en patrones), COBOL, PL/SQL, T-SQL, VB.NET, .Net Assembly, VB, C/C++, ASP .NET 1.x, ASP .NET 2.x, WSDL y C#. Cuando añada una nueva extensión, identifique si los archivos con la nueva extensión se pueden escanear, considerar como un archivo web o si se deben excluir.

Los valores en esta página son globales. Para establecer extensiones de archivo para proyectos individuales, utilice el separador de "Extensiones de archivo" en la página 261 de la vista Propiedades del proyecto seleccionado.

### Valores de extensión de archivo

Tabla 10. Valores de extensión de archivo

| Valor               | Descripción                                                           | Ejemplos de utilización                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Escanear o Asesorar | Incluir archivos con la extensión indicada en los análisis completos. | <ul style="list-style-type: none"><li>• Si se crea una extensión .xxx para proyectos Java y se marca como <b>Escanear</b> o <b>Asesorar</b>, los archivos que tengan esta extensión se compilarán y escanearán.</li><li>• Un archivo puede ser parte de un proyecto y no ser marcado como <b>Escanear</b> o <b>Asesorar</b> si no se debe compilar ni escanear (como por ejemplo, archivos de cabecera en C++). Estos archivos se deberían incluir en el proyectos, y se debería buscar en ellos durante el análisis basado en patrones.</li></ul> |

Tabla 10. Valores de extensión de archivo (continuación)

| Valor              | Descripción                                                                                                                                            | Ejemplos de utilización                                                                                                                                                                                                                                                                          |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Archivo web</b> | Marca los archivos con la extensión indicada para la compilación de JSP. Este valor permite que AppScan Source separe orígenes web de orígenes no web. | Si se crea una extensión .yyy para proyectos Java y se marca como un <b>Archivo web</b> , los archivos que tengan esta extensión se organizarán como orígenes web en los proyectos. Cuando AppScan Source prepare el análisis, estos archivos serán precompilados en clases para ser analizados. |
| <b>Excluir</b>     | No crear archivos de origen en el proyecto para archivos con la extensión indicada. No se escanearán los archivos con esta extensión.                  | Cree una extensión .zzz para los archivos que son necesarios para la compilación de proyectos, pero que no se necesitan incluir en el análisis.                                                                                                                                                  |

---

## Capítulo 4. Escaneo de código fuente y gestión de asesoramientos

En esta sección se explica cómo escanear el código fuente y gestionar asesoramientos.

Cuando haya configurado las aplicaciones y los proyectos, o si utiliza Application Discovery Assistant para crear las aplicaciones y los proyectos automáticamente, estará listo para escanear el código fuente. El resultado de un escaneo, un *asesoramiento*, se puede guardar o publicar. Un *asesoramiento guardado* es un archivo de resultados de escaneo guardado localmente que se puede publicar, abrir posteriormente para una selección adicional, o abrir en AppScan Source for Development. Un *asesoramiento publicado* consta de los resultados del escaneo guardados en AppScan Enterprise Server.

Los asesoramientos se gestionan en dos vistas:

- Mis asesoramientos
- Asesoramientos publicados

**Nota:** Cuando se guarda, publica o abre un asesoramiento, aparece el progreso en la barra de estado.

---

### Escaneo de código fuente

En esta tarea se describen los distintos métodos para iniciar escaneos.

#### Acerca de esta tarea

Puede escanear a varios niveles (todas las aplicaciones, una o varias aplicaciones, uno o varios proyectos, o uno o varios archivos). Si ha completado un escaneo, puede volver a realizarlo siempre que su asesoramiento esté abierto.

- “Escaneo de todas las aplicaciones” en la página 110
- “Escaneo de una o varias aplicaciones” en la página 110
- “Escaneo de uno o varios proyectos” en la página 110
- “Escaneo de uno o varios archivos” en la página 111
- “Volver a escanear código” en la página 111

Consulte “Consideraciones de escaneo” en la página 111 para obtener información sobre las consideraciones específicas del sistema operativo, consideraciones específicas del idioma, u otras restricciones que puedan afectar a los escaneos.

Cuando se escanea, siempre se utiliza una configuración de escaneo. Si establece una configuración de escaneo predeterminada y, a continuación, la suprime, la configuración de escaneo incorporada **Escaneo normal** se utilizará de forma silenciosa al escanear. Para obtener más información sobre las configuraciones de escaneo, consulte “Gestión de las configuraciones de escaneo” en la página 113 y las descripciones de las opciones de escaneo que se indican a continuación:

## Escaneo de todas las aplicaciones

### Procedimiento

Realice una de estas acciones:

1. Seleccione **Escanear > Escanear todo** en el menú principal del espacio de trabajo. El escaneo se ejecutará con la configuración de escaneo predeterminada.
2. En la vista Explorador:
  - Pulse con el botón derecho en **Todas las aplicaciones** y luego seleccione **Escanear todas las aplicaciones** en el menú. El escaneo se ejecutará con la configuración de escaneo predeterminada.
  - Para utilizar una configuración de escaneo diferente para el escaneo, pulse con el botón derecho en **Todas las aplicaciones** y luego seleccione **Escanear todas las aplicaciones con** en el menú. Seleccione la configuración de escaneo que desee utilizar. O bien, para establecer una configuración de escaneo predeterminada diferente, seleccione la acción **Editar configuraciones** (en la vista Configuración del escaneo, seleccione la configuración que desea establecer como valor predeterminado y, a continuación, pulse **Seleccionar como valor predeterminado**).

## Escaneo de una o varias aplicaciones

### Procedimiento

1. En la vista Explorador, seleccione una o varias aplicaciones.
2. Realice una de estas acciones:
  - a. Seleccione **Escanear > Escanear selección** en el menú principal del espacio de trabajo. El escaneo se ejecutará con la configuración de escaneo predeterminada.
  - b. En la vista Explorador:
    - Pulse con el botón derecho en la selección y elija **Escanear aplicación** en el menú. El escaneo se ejecutará con la configuración de escaneo predeterminada.
    - Para utilizar una configuración de escaneo diferente para el escaneo, pulse con el botón derecho en la selección y luego seleccione **Escanear aplicación con** en el menú. Seleccione la configuración de escaneo que desee utilizar. O bien, para establecer una configuración de escaneo predeterminada diferente, seleccione la acción **Editar configuraciones** (en la vista Configuración del escaneo, seleccione la configuración que desea establecer como valor predeterminado y, a continuación, pulse **Seleccionar como valor predeterminado**).

## Escaneo de uno o varios proyectos

### Procedimiento

1. En la vista Explorador, seleccione uno o varios proyectos.
2. Realice una de estas acciones:
  - a. Seleccione **Escanear > Escanear selección** en el menú principal del espacio de trabajo. El escaneo se ejecutará con la configuración de escaneo predeterminada.
  - b. En la vista Explorador:
    - Pulse con el botón derecho en la selección y elija **Escanear proyecto** en el menú. El escaneo se ejecutará con la configuración de escaneo predeterminada.

- Para utilizar una configuración de escaneo diferente para el escaneo, pulse con el botón derecho en la selección y luego seleccione **Escanear proyecto con** en el menú. Seleccione la configuración de escaneo que desee utilizar. O bien, para establecer una configuración de escaneo predeterminada diferente, seleccione la acción **Editar configuraciones** (en la vista Configuración del escaneo, seleccione la configuración que desea establecer como valor predeterminado y, a continuación, pulse **Seleccionar como valor predeterminado**).

## Escaneo de uno o varios archivos

### Procedimiento

1. En la vista Explorador, seleccione uno o varios archivos.
2. Realice una de estas acciones:
  - a. Seleccione **Escanear > Escanear selección** en el menú principal del espacio de trabajo. El escaneo se ejecutará con la configuración de escaneo predeterminada.
  - b. En la vista Explorador:
    - Pulse con el botón derecho en la selección y elija **Escanear archivo** en el menú. El escaneo se ejecutará con la configuración de escaneo predeterminada.
    - Para utilizar una configuración de escaneo diferente para el escaneo, pulse con el botón derecho en la selección y luego seleccione **Escanear archivo con** en el menú. Seleccione la configuración de escaneo que desee utilizar. O bien, para establecer una configuración de escaneo predeterminada diferente, seleccione la acción **Editar configuraciones** (en la vista Configuración del escaneo, seleccione la configuración que desea establecer como valor predeterminado y, a continuación, pulse **Seleccionar como valor predeterminado**).

## Volver a escanear código

### Procedimiento

Para volver a escanear el destino actual, seleccione **Escanear > Escanear de nuevo** en el menú principal. La última configuración de escaneo que se ha utilizado para escanear el elemento (o los elementos seleccionados) se utilizará de nuevo para el escaneo:

- Si se ha utilizado la configuración de escaneo predeterminada para el escaneo anterior y si se ha establecido un nuevo escaneo predeterminado, se utilizará la nueva configuración de escaneo predeterminada para el escaneo.
- Si se ha utilizado una configuración de escaneo distinta de la predeterminada para el escaneo anterior, se utilizará para el escaneo. Si esa configuración de escaneo se ha modificado y guardado desde el escaneo anterior, se utilizará la configuración de escaneo modificada.

## Consideraciones de escaneo

Este tema describe restricciones y consideraciones que pueden afectar a los escaneos.

- “General” en la página 112
- “Windows” en la página 112
- “Linux” en la página 112
- “Java” en la página 112

## General

**Restricción:** Cuando realice un escaneo de varias aplicaciones o proyectos, se crea un nodo padre que contiene asesoramientos para cada elemento escaneado en la vista Mis asesoramientos. Los asesoramientos hijo individuales no se pueden gestionar en este caso (por ejemplo, los asesoramientos hijo no se pueden eliminar o publicar de forma individual). Cuando varias aplicaciones o proyectos se escanean a la vez, solo podrá gestionar los asesoramientos como un grupo (el nodo padre).

**Importante:** Si está trabajando con un proyecto AppScan Source que tiene dependencias en un entorno de desarrollo, por ejemplo, un proyecto de IBM MobileFirst Platform, asegúrese de que crea el proyecto en el entorno de desarrollo antes de importarlo. Después de importar el proyecto, si modifica los archivos que contiene, asegúrese de que vuelve a crearlo en el entorno de desarrollo antes del escaneo en AppScan Source. Si no lo hace, AppScan Source omite las modificaciones que se realicen en los archivos.

## Windows

La posibilidad de escanear archivos individuales o de selección múltiple no está disponible para los archivos de Microsoft (por ejemplo, .cs y .vbnet).

## Linux

El cliente de AppScan Source for Analysis se basa en Eclipse. En Linux, Eclipse requiere la instalación de un componente de terceros para poder mostrar contenido basado en navegador. Sin este componente, AppScan Source for Analysis puede mostrar síntomas como bloqueos después del inicio de sesión o un error durante la utilización del producto. Consulte el apartado “Habilitación de contenido basado en un navegador en Linux para AppScan Source for Analysis” en la página 126 para obtener más información.

## Java

**Consejo:** Si está escaneando Java y faltan dependencias en el proyecto de Java, AppScan Source creará rastreos sintetizando las partes que las dependencias hayan proporcionado. Esta síntesis puede que no refleje de forma precisa la información en archivos .jar. Para limitar la síntesis y mejorar la precisión de los resultados, puede especificar las dependencias que faltan, como por ejemplo:

1. Tras escanear, abra <data\_dir>\logs\scanner\_exceptions.log (donde <data\_dir> es la ubicación de los datos de programa AppScan Source, como se describe en “Instalación y ubicaciones de archivo de datos de usuario” en la página 335) para ver si a AppScan Source le faltan dependencias de las que se ha informado.
2. Modifique las propiedades de proyecto para que incluyan las dependencias. Para ello, siga las instrucciones de “Modificación de las propiedades del proyecto y de la aplicación” en la página 83 y, a continuación, especifique y guarde las dependencias en el separador **Dependencias del proyecto JSP** o **Dependencias del proyecto**.
3. Vuelva a escanear el proyecto.

**Nota:** De forma predeterminada, AppScan Source escanea archivos Java y código de bytes de Java con dependencias o errores de compilación perdidos. Estos valores se pueden modificar como se indica a continuación:



1. Abra <data\_dir>\config\scan.ozsettings en un editor de textos.
2. Para cambiar el valor de error de compilación, ubique `compile_java_sources_with_errors` en el archivo. Este valor es similar a:
 

```
<Setting
  name="compile_java_sources_with_errors"
  value="true"
  default_value="true"
  type="bool"
  hidden="true"
  display_name="compile_java_sources_with_errors"
  description="Intento de escanear código java con errores de compilación".
/>
```
3. Para modificar el valor de dependencia que falta, ubique `scan_java_bytecode_without_dependencies` en el archivo. Este valor es similar a:
 

```
<Setting
  name="scan_java_bytecode_without_dependencies"
  value="true"
  default_value="true"
  type="bool"
  hidden="true"
  display_name="scan_java_bytecode_without_dependencies"
  description="Escanea el código de bytes de Java incluso cuando algunas de
    las dependencias faltan mediante la sintetización artificial
    de los símbolos no resueltos".
/>
```
4. En el valor, modifique el atributo `value`. Si el atributo se establece en `true`, este valor estará activo. Si el valor de error de compilación está establecido en `false`, AppScan Source omitirá el código Java con errores de compilación durante los escaneos. Si el valor de dependencia que falta está establecido en `false`, AppScan Source no escaneará el código de bytes Java si faltan dependencias.
5. Guarde el archivo una vez que haya modificado este valor e inicie o reinicie AppScan Source.

## Gestión de las configuraciones de escaneo

Las configuraciones de escaneo se utilizan cuando se inician escaneos. En una configuración de escaneo, puede especificar las reglas de origen que se utilizan durante un escaneo. Los valores establecidos en una configuración de escaneo a menudo pueden mejorar los resultados del escaneo, y la posibilidad de guardar estos valores facilita el escaneo y permite ahorrar tiempo.

### Acerca de esta tarea

En esta tarea se describen los pasos necesarios para gestionar las configuraciones de escaneo.

- “Creación de una configuración de escaneo” en la página 114
- “Modificación de una configuración de escaneo” en la página 117
- “Eliminación de una configuración de escaneo” en la página 117
- “Compartimiento de configuraciones de escaneo y trabajo con configuraciones compartidas” en la página 118
- “Establecimiento de las configuraciones de escaneo como valor predeterminado” en la página 118
- “Configuraciones de escaneo incorporadas” en la página 119

Las configuración de escaneo se gestionan en la “Vista Configuración del escaneo” en la página 119. Para abrir esta vista, seleccione **Ver > Configuración del escaneo** en la barra de menús principal, o seleccione la acción **Editar configuraciones** en la vista Explorador.

Una vez aplicadas las configuraciones de escaneo, puede utilizarlas cuando inicie escaneos en AppScan Source for Analysis (consulte “Escaneo de código fuente” en la página 109 para obtener más información). También puede utilizar las configuraciones de escaneo cuando inicia escaneos en AppScan Source for Automation, AppScan Source for Development y la interfaz de línea de mandatos (CLI) de AppScan Source.

## Creación de una configuración de escaneo

### Procedimiento

1. Realice una de estas acciones:
  - a. Pulse el botón **Nuevo** de la vista Configuración del escaneo.
  - b. Seleccione una configuración existente en la lista y, a continuación, pulse **Duplicar**. Se creará una configuración de escaneo basada en los valores de la configuración de escaneo original, que puede modificar y guardar como una nueva configuración.
2. En el separador **General**, sección **Información básica**:
  - a. Especifique un nombre exclusivo para la configuración en el campo **Nombre**. Tenga en cuenta que, en una configuración de escaneo, la especificación de un nombre exclusivo es el único valor obligatorio y el resto de los valores son opcionales.
  - b. Opcional: Especifique una descripción para la configuración de escaneo.
3. Opcional: Utilice el separador **General**, sección **Información de filtros** para establecer los filtros para el escaneo. Para obtener más información sobre los filtros, consulte “Selección con filtros” en la página 151. En esta sección, puede elegir uno o varios filtros para aplicar al escaneo, siempre que se utilice la configuración de escaneo. Al seleccionar un filtro, puede elegir un AppScan Source filtro predefinido o un filtro compartido o uno que haya creado. En esta sección:
  - a. Pulse **Añadir** y, a continuación, en el recuadro de diálogo Seleccionar filtro, elija el filtro o filtros que desee añadir. Cuando se selecciona un filtro, sus rasgos aparecerán como sólo lectura en el lado derecho del recuadro de diálogo. Pulse en **Aceptar** para añadir el filtro o filtros a la configuración de escaneo.

#### Nota:

- Para aplicar lo inverso del filtro a la configuración de escaneo, seleccione el recuadro de selección **Invertir filtro** antes de pulsar en **Aceptar**.
- Cuando se encuentre en el recuadro de diálogo Seleccionar filtro, puede multiseleccionar más de un filtro para añadir. Si está seleccionado el recuadro de selección **Invertir filtro** cuando lo hace, se añadirá lo inverso de todos los filtros seleccionados a la configuración de escaneo.

Una vez que salga del recuadro de diálogo Seleccionar filtro, el filtro o filtros aparecerán en la lista y la columna **Invertido** indicará si se ha invertido el filtro.

- b. Para eliminar filtros que se hayan añadido, seleccione o multiseccione los filtros y, a continuación, pulse **Eliminar**.

- c. Los filtros de exclusión contienen reglas para qué tipos de vulnerabilidad, interfaces de programación de aplicaciones (API), archivos, directorios, proyectos o reglas de rastreo se eliminen de los resultados. Si incluye varios filtros de exclusión en una configuración de escaneo, es posible que entren en conflicto entre sí y afecten a los resultados. Por ejemplo, dados estos dos filtros:

- El Filtro 1 elimina todos los resultados del tipo de vulnerabilidad `Validation.EncodingRequired`. No está invertido de forma que estos resultados se excluirán del asesoramiento.
- El Filtro 2 elimina todos los resultados del tipo de vulnerabilidad `Validation.Required`. No está invertido de forma que estos resultados se excluirán del asesoramiento.

Si ambos filtros se aplican utilizando una configuración de escaneo, de forma predeterminada se descartarán entre sí. El Filtro 1 excluirá los resultados `Validation.EncodingRequired`, pero incluirá los resultados `Validation.Required`. El Filtro 2 excluirá los resultados `Validation.Required`, pero incluirá los resultados `Validation.EncodingRequired`. El resultado final será que se incluirán los resultados `Validation.EncodingRequired` y `Validation.Required`.

Para eliminar los resultados de *cualquier* filtro excluido especificado, seleccione **Coincidencia de cualquier filtro de exclusión no invertido**. Con el ejemplo anterior, si se selecciona este recuadro de selección, todos los resultados `Validation.EncodingRequired` y `Validation.Required` se excluirán del asesoramiento.

4. Opcional: Utilice el separador **Análisis de flujo corrupto**, sección **Análisis de flujo corrupto** para permitir el análisis de flujo corrupto. Seleccionado de forma predeterminada, **Análisis de flujo corrupto** es el tipo de análisis primario realizado por AppScan Source. Cuando inicie un escaneo, el análisis de flujo corrupto produce rastros de flujo de datos que le permiten determinar mejor las vulnerabilidades. Puede establecer el **Ámbito** del análisis como se indica a continuación:
- **Ámbito de Aplicación:** el análisis de flujo corrupto se realizará entre proyectos de una aplicación y archivos de un proyecto.
  - **Ámbito de Proyecto:** el análisis de flujo corrupto se realizará entre archivos de un proyecto.
  - **Ámbito de Archivo:** el análisis de flujo corrupto se realizará en cada archivo por separado.

**Nota:** Las configuraciones del separador **Análisis de flujo corrupto** no se aplican al escanear JavaScript, ColdFusion, Perl, Cobol, PL/SQL ni T-SQL.

5. Opcional: El separador **Análisis de flujo corrupto**, sección **Reglas de escaneo** le permite especificar las reglas de origen que se aplicarán para el escaneo (consulte “Separador Análisis de flujo corrupto” en la página 120 para obtener más información). En esta sección, puede escanear con conjuntos de reglas de origen seleccionados o puede seleccionar propiedades de regla individuales para utilizarlas en el escaneo:
- a. De forma predeterminada, esta sección permite elegir los conjuntos de reglas que desea aplicar. Seleccione uno o varios de los cuadros de selección de conjuntos de reglas disponibles.
  - b. Para elegir reglas individuales en lugar de conjuntos de reglas, pulse **Descartar los conjuntos de reglas seleccionados y permitir seleccionar propiedades de regla individuales**. Esto abre el cuadro de diálogo **Seleccionar propiedades de reglas**, que le permite seleccionar las

propiedades de la regla individual. Si se rellena este cuadro de diálogo, se descartarán los conjuntos de reglas que se hayan seleccionado. Las reglas de escaneo que tienen seleccionadas propiedades de regla se utilizarán para el escaneo.

Si elige propiedades de regla individuales para el escaneo y prefiere seleccionar conjuntos de reglas, pulse **Descartar las propiedades de la regla seleccionada y permitirme seleccionar por conjunto de reglas**. Se descartarán las propiedades de regla que se hayan seleccionado en el cuadro de diálogo Seleccionar propiedades de reglas, para que pueda seleccionar los conjuntos de regla que desee.

**Nota:**

- Al seleccionar propiedades de reglas individuales, los elementos seleccionados se aplican a las propiedades de los orígenes y no a las de los receptores ("sink"). Esto significa que está limitando la superficie de ataque únicamente a aquellos orígenes que tienen las propiedades seleccionadas. Podría ver en sus resultados vulnerabilidades que no coincidiesen con las propiedades seleccionadas, puesto que los tipos de vulnerabilidad se basan en el receptor ("sink") y no en el origen.
  - Las configuraciones del separador **Análisis de flujo corrupto** no se aplican al escanear JavaScript, ColdFusion, Perl, Cobol, PL/SQL ni T-SQL.
6. Opcional: El separador **Análisis de flujo corrupto**, sección **Valores avanzados** está pensada sólo para usuarios avanzados. Contiene una amplia variedad de valores que pueden mejorar los resultados del escaneo. El texto flotante describe cada valor de esta sección.

**Nota:** Las configuraciones del separador **Análisis de flujo corrupto** no se aplican al escanear JavaScript, ColdFusion, Perl, Cobol, PL/SQL ni T-SQL.

7. Opcional: Los valores del separador **Análisis de patrón** le permiten habilitar y establecer reglas para el escaneo basado en patrones. El escaneo basado en patrones es un análisis del código fuente basado en criterios de búsqueda personalizados. Consulte el apartado "Personalización con reglas basadas en patrón" en la página 247 para obtener más información. Para habilitar el escaneo basado en patrones, seleccione el recuadro de selección **Análisis de patrones**. Cuando lo haga, se habilitarán las secciones **Conjuntos de reglas de patrón** y **Reglas de patrón**:
- a. Para añadir un conjunto de reglas, pulse **Añadir** en la sección **Conjuntos de reglas de patrón**. Esto abre el recuadro de diálogo Añadir conjuntos de reglas de patrón, que le permite seleccionar uno o varios conjuntos de reglas. Al seleccionar un conjunto de reglas, las reglas que contiene se mostrarán en el lado derecho del recuadro de diálogo, y los tipos de proyecto a los que se aplica el conjunto de reglas se listarán en el campo **Tipos de proyecto**. Pulse en **Aceptar** para añadir los conjuntos de reglas seleccionados.
  - b. Para añadir una regla, pulse **Añadir** en la sección **Reglas de patrón**. Esto abre el recuadro de diálogo Añadir patrón, que le permite seleccionar una o varias reglas. También puede pulsar **Crear regla nueva** para crear una regla nueva (consulte "Creación de una regla de patrón" en la página 251). Si crea una regla nueva, se añadirá a la lista y se seleccionará. Tras seleccionar o crear reglas, pulse en **Aceptar** para añadirlas a la configuración de escaneo.

**Consejo:** En el recuadro de diálogo Añadir reglas de patrón, la ayuda emergente indica las expresiones utilizadas para cada regla.

**Nota:**

- Al añadir un conjunto de reglas, las reglas de cada conjunto de reglas se filtrarán fuera del recuadro de diálogo Añadir reglas de patrón.
  - Si añade una regla y, a continuación, añade un conjunto de reglas que también incluye dicha regla, la sección Reglas de patrón enumerará la regla con una indicación que se incluye en un conjunto de reglas. Debido a que esta regla ya está incluida en un conjunto de reglas, si intenta eliminar la regla individual, sólo se eliminará de la sección Reglas de patrón y no de la configuración de escaneo. Para eliminar la regla de la configuración de escaneo, elimine el conjunto de reglas o modifíquela para que no incluya la regla.
- c. Cualquier regla o conjunto de reglas que añada se puede eliminar utilizando el botón **Eliminar** o efectuando una pulsación con el botón derecho y seleccionando **Eliminar**. También puede multiseleccionar reglas y conjuntos de reglas al utilizar esta acción.

**Nota:** Si una configuración de escaneo incluye reglas o conjuntos de reglas que se eliminan posteriormente de la base de datos de vulnerabilidad, la próxima vez que abra la configuración de escaneo, las reglas o conjuntos de reglas aparecerán con un mensaje que indica que no existen. Las acciones **Eliminar** no estarán disponibles para estas reglas o conjuntos de reglas; sin embargo, la próxima vez que guarde la configuración de escaneo, se eliminarán automáticamente.

8. Una vez definidos todos los valores en la configuración del escaneo, pulse **Guardar**.

## **Modificación de una configuración de escaneo**

### **Procedimiento**

1. En la vista Configuración del escaneo, seleccione la configuración de escaneo que desee modificar.

**Nota:** Para compartir configuraciones de escaneo, o para modificar o suprimir una configuración de escaneo compartida, debe tener permiso para **Gestionar configuraciones compartidas**. Para obtener información sobre cómo establecer permisos, consulte el manual *IBM Security AppScan Source Guía de instalación y administración*.

**Nota:** No puede modificar “Configuraciones de escaneo incorporadas” en la página 119.

2. Después de modificar la configuración del escaneo, pulse **Guardar**.

## **Eliminación de una configuración de escaneo**

### **Procedimiento**

1. En la vista Configuración del escaneo, seleccione la configuración de escaneo que desee eliminar.

**Nota:** No puede eliminar “Configuraciones de escaneo incorporadas” en la página 119.

2. Pulse **Suprimir**.

## Compartimiento de configuraciones de escaneo y trabajo con configuraciones compartidas

### Acerca de esta tarea

Las configuraciones de escaneo pueden guardarse en base de datos de AppScan Source para compartirlas con otros usuarios. Para compartir una configuración de escaneo con otras personas, pulse **Compartir**.

**Nota:** Para compartir configuraciones de escaneo, o para modificar o suprimir una configuración de escaneo compartida, debe tener permiso para **Gestionar configuraciones compartidas**. Para obtener información sobre cómo establecer permisos, consulte el manual *IBM Security AppScan Source Guía de instalación y administración*.

Las configuraciones de escaneo que se han compartido con otros usuarios aparecen en la lista de configuraciones de escaneo.

#### Nota:

- Cuando se ha compartido una configuración de escaneo, no se puede eliminar el compartimiento. En su lugar, puede realizar una de estas tareas:
  - Suprima la configuración de escaneo compartida. De esta forma, se suprimirá en el servidor.
  - Duplique la configuración de escaneo compartida y, a continuación, suprimala. La duplicación de la configuración de escaneo creará una copia idéntica de ella.
- Si está compartiendo una configuración de escaneo que contiene filtros ya compartidos, la acción de compartir se completará sin ninguna indicación. Si, no obstante, está compartiendo una configuración de escaneo que contiene filtros que ha creado de forma local, una solicitud le hará saber que los filtros también se compartirán. Podrá cancelar la acción de compartir de la configuración de escaneo si no desea compartir los filtros locales.
- No puede modificar ni guardar configuraciones de escaneo compartidas añadiendo filtros locales. Para añadir estos filtros a una configuración de escaneo compartida, comparta los filtros y, a continuación, añádalos a la configuración de escaneo compartida.
- Si tiene permiso para **Gestionar configuraciones compartidas** pero no permiso para **Gestionar filtros compartidos**, no podrá compartir una configuración de escaneo que contiene filtros locales.

## Establecimiento de las configuraciones de escaneo como valor predeterminado

### Acerca de esta tarea

Puede establecer una configuración de escaneo como el valor predeterminado, ya sea local, incorporada o compartida. Si establece una configuración de escaneo compartida como valor predeterminado, sólo se aplica localmente y no afecta a otros usuarios. Cuando se escanea, siempre se utiliza una configuración de escaneo. Si establece una configuración de escaneo predeterminada y, a continuación, la suprime, la configuración de escaneo incorporada **Escaneo normal** se utilizará de forma silenciosa al escanear.

Para obtener más información sobre cómo se utiliza la configuración de escaneo predeterminada, consulte “Escaneo de código fuente” en la página 109.

## Procedimiento

1. En la vista Configuración del escaneo, seleccione la configuración de escaneo que desee establecer como valor predeterminado.
2. Pulse **Seleccionar como valor predeterminado**.

## Configuraciones de escaneo incorporadas Acerca de esta tarea

AppScan Source proporciona configuraciones de escaneo incorporadas. Estas no se pueden modificar ni eliminar. Si las selecciona en la lista, podrá duplicarlas o ver sus valores.

## Vista Configuración del escaneo

La vista Configuración del escaneo le permite crear configuraciones que puede utilizar al iniciar escaneos. También puede utilizar la vista para establecer una configuración de escaneo predeterminada. En una configuración de escaneo, puede especificar las reglas de origen que se utilizan durante un escaneo y puede incluir varios valores de escaneo. Los valores establecidos en una configuración de escaneo a menudo pueden mejorar los resultados del escaneo, y la posibilidad de guardar estos valores facilita el escaneo y permite ahorrar tiempo.

La vista Configuración del escaneo tiene estas secciones principales:

- “Gestión de la configuración de escaneo”
- “Separador General” en la página 120
- “Separador Análisis de flujo corrupto” en la página 120
- “Separador Análisis de patrones” en la página 121

## Gestión de la configuración de escaneo

Utilice esta sección para seleccionar, añadir, eliminar, guardar y compartir configuraciones de escaneo, así como para establecer configuraciones de escaneo predeterminadas.

- Para crear una nueva configuración de escaneo, pulse **Nueva**. Después de completar los valores de la configuración de escaneo, pulse **Guardar** para guardar los cambios. Para establecer la configuración de escaneo como el valor predeterminado, pulse **Seleccionar como valor predeterminado** después de guardarla. Para obtener más información sobre cómo se utiliza la configuración de escaneo predeterminada, consulte “Escaneo de código fuente” en la página 109.
- Para trabajar con una configuración de escaneo existente, selecciónela en la lista:
  - Si modifica los valores de la configuración de escaneo, pulse **Guardar** para guardar los cambios (para descartar los cambios no deseados, cambie a otra configuración de escaneo y pulse **Descartar**).
  - Para eliminar la configuración de escaneo seleccionada, pulse **Suprimir**.
  - Para duplicar la configuración de escaneo, pulse **Duplicar**. Se creará una nueva configuración de escaneo basada en los valores de la configuración de escaneo original.
  - Para establecer la configuración de escaneo como el valor predeterminado, pulse **Seleccionar como valor predeterminado**. Para obtener más información sobre cómo se utiliza la configuración de escaneo predeterminada, consulte “Escaneo de código fuente” en la página 109.

- Para compartir la configuración de escaneo con otras personas, pulse **Compartir**. La configuración de escaneo se guardará en base de datos de AppScan Source.

**Nota:** Para compartir configuraciones de escaneo, o para modificar o suprimir una configuración de escaneo compartida, debe tener permiso para **Gestionar configuraciones compartidas**. Para obtener información sobre cómo establecer permisos, consulte el manual *IBM Security AppScan Source Guía de instalación y administración*.

**Nota:** AppScan Source proporciona configuraciones de escaneo incorporadas. Estas no se pueden modificar ni eliminar. Si las selecciona en la lista, podrá duplicarlas o ver sus valores.

## Separador General

### Información básica

Esta sección permite nombrar configuraciones de escaneo y proporcionar descripciones.

### Filtros

En esta sección, puede elegir uno o varios filtros para aplicar al escaneo, siempre que se utilice la configuración de escaneo. Al seleccionar un filtro, puede elegir un AppScan Source filtro predefinido o un filtro compartido o uno que haya creado. Consulte “Gestión de las configuraciones de escaneo” en la página 113 para ver más detalles.

## Separador Análisis de flujo corrupto

### Análisis de flujo corrupto

Habilite y establezca el ámbito del análisis de flujo corrupto.

### Reglas de escaneo

Utilice esta sección para determinar qué reglas de origen se aplicarán en el escaneo.

Un origen es una entrada para el programa, como un archivo, una solicitud de servlet, una entrada de consola o un socket. Al excluir algunas reglas de origen, puede acelerar el escaneo y evitar la detección de vulnerabilidades debidas a entradas que no son de interés.

Las reglas se etiquetan con propiedades de reglas para indicar que están relacionadas con una determinada vulnerabilidad, mecanismo, atributo o tecnología. Estas propiedades se agrupan en conjuntos de reglas, que se corresponden con un conjunto común de reglas relacionadas. Puede limitar las reglas de origen incluidas en el escaneo mediante la especificación de conjuntos de reglas o propiedades de reglas individuales.

- Seleccione uno o varios tipos de vulnerabilidad (organizados por tipo en los conjuntos de reglas) que desee incluir en el escaneo:
  - **Todo:** si selecciona esta opción, se detectarán las vulnerabilidades debidas a todos los orígenes de entrada soportados.



- **Entrada de usuario:** si selecciona esta opción, se detectarán las vulnerabilidades debidas a la entrada del usuario final.
- **Aplicaciones web:** si selecciona esta opción, se detectarán las vulnerabilidades debidas al riesgo de las aplicaciones web.
- **Registro y manejo de errores:** si selecciona esta opción, se detectarán las vulnerabilidades debidas a los mecanismos de registro y manejo de errores.
- **Entorno:** si selecciona esta opción, se detectarán las vulnerabilidades debidas a los archivos de configuración, los archivos del entorno del sistema y los archivos de propiedades.
- **Sistemas externos:** si selecciona esta opción, se detectarán las vulnerabilidades debidas a las entidades externas.
- **Almacén de datos:** si selecciona esta opción, se detectarán las vulnerabilidades debidas a los almacenes de datos (por ejemplo, las bases de datos y la memoria caché).
- **Elementos poco usuales:** si selecciona esta opción, se detectarán las vulnerabilidades debidas a las rutinas que no forman parte normalmente de una aplicación de producción.
- **Sistema de archivos:** si selecciona esta opción, se detectarán las vulnerabilidades debidas a los sistemas de archivos.
- **Datos confidenciales:** si selecciona esta opción, se detectarán las vulnerabilidades debidas a los datos confidenciales.

El texto flotante describe cada conjunto de reglas de esta sección.

- Seleccione las propiedades de las reglas de escaneo individuales que desee incluir en el escaneo: pulse **Descartar los conjuntos de reglas seleccionados y permitir seleccionar propiedades de regla individuales**. Esto abre el cuadro de diálogo Seleccionar propiedades de reglas, que le permite seleccionar las propiedades de la regla individual. Si se rellena este cuadro de diálogo, se descartarán los conjuntos de reglas que se hayan seleccionado. Las reglas de escaneo que tienen seleccionadas propiedades de regla se utilizarán para el escaneo.

## Valores avanzados

Esta sección está especialmente indicada para usuarios avanzados. Contiene una amplia variedad de valores que pueden mejorar los resultados del escaneo. El texto flotante describe cada valor de esta sección.

## Separador Análisis de patrones

### análisis de patrón

Utilice esta sección para habilitar el escaneo basado en patrones cuando se utilice la configuración de escaneo. El escaneo basado en patrones es un análisis del código fuente basado en criterios de búsqueda personalizados.

### Conjuntos de reglas de patrón y Reglas de patrón

Utilice estas secciones para añadir reglas y conjuntos de reglas a utilizar durante el análisis de patrones. Consulte los apartados “Personalización con reglas basadas en patrón” en la página 247 y “Gestión de las configuraciones de escaneo” en la página 113 para obtener más información.

## Análisis incremental para Java

Cuando se habilita el escaneo incremental, AppScan Source coloca en la caché los datos de análisis. Cuando se vuelve a escanear un proyecto o aplicación, AppScan Source utiliza estos datos para determinar los cambios de código de forma que únicamente se analizan de nuevo las partes del código afectadas por los cambios. El resultado es un análisis completo del código, pero en una fracción del tiempo.

### Acerca de esta tarea

Se da soporte al análisis incremental en Windows y Linux. Cuando se habilita, el análisis incremental se realiza en aplicaciones o proyectos de AppScan Source - o en espacios de trabajo o proyectos de Eclipse. Después de habilitar el análisis incremental, el primer escaneo que ejecute en relación a su proyecto, aplicación o espacio de trabajo será siempre un escaneo completo (la caché de análisis de vulnerabilidad únicamente se actualiza durante un escaneo completo). Esto permite que AppScan Source coloque en la caché datos para escaneos posteriores. Los escaneos posteriores de sus proyectos, aplicaciones o espacios de trabajo son escaneos incrementales, en la medida que no se haya borrado la caché de análisis de vulnerabilidad, y en la medida que el número de archivos cambiados no supere un umbral configurable.

Siga los siguientes pasos para habilitar y utilizar el análisis incremental:

### Procedimiento

1. Abra <dir\_datos>\config\scan.ozsettings en un editor de texto (donde <data\_dir> es la ubicación de los datos de programa AppScan Source, como se describe en “Instalación y ubicaciones de archivo de datos de usuario” en la página 335). Encuentre el valor incremental\_analysis en el archivo. Este valor es similar a:

```
<Setting
  name="incremental_analysis"
  read_only="false"
  default_value="false"
  description="Attempt to scan only changed files,
    instead of re-scanning everything."
  type="bool"
  value="false"
  display_name="Incremental Analysis"
  hidden="true"
/>
```

En este valor, modifique el atributo value. Si el atributo se establece en true, este valor estará activo. Si se establece en false, AppScan Source no realizará el escaneo incremental al escanear.

2. En <dir\_datos>\config\scan.ozsettings, encuentre el valor percentage\_of\_files\_changed:

```
<Setting
  name="percentage_of_files_changed"
  read_only="false"
  default_value="50"
  description="In incremental scanning, if percentage of files
    being changed since last scan exceeds the threshold, full
    scan will be initiated. The percentage ranges from 0 to 100.
    Default threshold is 50, which represents 50%."
  type="int"
  value="50"
  display_name="Percentage of files being changed"
  hidden="true"
/>
```

Este valor sirve para especificar el porcentaje de archivos cambiados antes de que se inicie un escaneo completo. De forma predeterminada, este porcentaje umbral es del 50%, lo que significa que si vuelve a escanear después de que se hayan modificado más del 50% de archivos en su proyecto, aplicación o espacio de trabajo, se iniciará un escaneo completo en lugar de un escaneo de análisis incremental. En este valor, cambie el atributo `value`, tal como desee, con su umbral de porcentaje preferido.

3. Guarde `<dir_datos>\config\scan.ozsettings` después de haber modificado todos los valores pertinentes y, a continuación, inicie o vuelva a iniciar el producto AppScan Source para dar soporte al análisis incremental. Por ejemplo, reinicie AppScan Source for Analysis, el Plugin AppScan Source for Development Eclipse o la interfaz de línea de mandatos (CLI) de AppScan Source - o reinicie el servicio AppScan Source for Automation.
4. Ahora, cuando vuelva a escanear aplicaciones o proyectos de Java con la misma configuración de escaneo, se realizará un análisis incremental si el número de archivos cambiados no supera el umbral y si no se ha borrado el caché de análisis de vulnerabilidad.
5. **Borrado de la caché de análisis de vulnerabilidad:** Si se presentan problemas en el escaneo incremental, o si desea realizar un análisis completo cuando está habilitado el análisis incremental, borre la caché de vulnerabilidad antes de escanear de nuevo:
  - AppScan Source for Analysis:
    - a. Abra la vista Propiedades de su proyecto de AppScan Source. Si está escaneando una aplicación, abra la vista propiedades de cualquier proyecto hijo (suprimiendo la caché del proyecto también suprimirá la caché de sus aplicaciones).
    - b. En el separador Visión general, pulse **Borrar memoria caché**.
  - Plugin AppScan Source for Development Eclipse : Suprima `<dir_datos>\temp\<espacio_trabajo>\<proyecto>`, donde:
    - `<data_dir>` es la ubicación de los datos de programa AppScan Source, como se describe en “Instalación y ubicaciones de archivo de datos de usuario” en la página 335.
    - `<espacio_trabajo>` es el nombre del espacio de trabajo de Eclipse en el que está escaneando. Para suprimir la caché de todo su espacio de trabajo, suprima todo el directorio `<dir_datos>\temp\<espacio_trabajo>`.
    - `<proyecto>` es el nombre del proyecto de Eclipse que está escaneando. Para suprimir la caché del proyecto, suprima el directorio `<dir_datos>\temp\<espacio_trabajo>\<proyecto>`.
  - La interfaz de línea de mandatos (CLI) de AppScan Source: Utilice el mandato `clearcache`, tal como se describe en *IBM Security AppScan Source Utilities Guía del usuario*.
  - AppScan Source for Automation: Utilice el argumento `-clearcache` del mandato de `ScanApplication`, tal como se describe en *IBM Security AppScan Source Utilities Guía del usuario*.

## Resultados

Después de escanear en AppScan Source for Analysis, puede utilizar la característica de **Diferencia entre asesoramientos** para comparar los asesoramientos antes y después de los cambios en el código.

### Consejo:

- Para forzar un escaneo de análisis completo, inhabilite el análisis incremental o borre la caché de análisis de vulnerabilidad.
- Al ejecutar análisis incrementales, debería ejecutar un escaneo de análisis completo después de realizar cualquiera de las siguientes modificaciones:
  - Cambios a las reglas de seguridad o cambios a las reglas personalizadas que se aplican al proyecto o aplicación.
  - Cambios de configuración de escaneo.
  - Cambios a los archivos .ozsettings que afecten a los escaneos.
  - Cambios a las propiedades del proyecto o la aplicación. Por ejemplo, los cambios realizados en la vista de Propiedades de AppScan Source for Analysis para Todas las aplicaciones o a un proyecto o aplicación seleccionados.
  - Añadir un nuevo proyecto a una aplicación o al suprimir un proyecto existente.
  - Excluir archivos de escaneos. Por ejemplo, en AppScan Source for Analysis, puede elegir excluir un archivo del escaneo pulsando con el botón derecho sobre el mismo en la vista de Explorador y elegir **Excluir de escaneos**.
- La información más actual sobre el análisis incremental se puede encontrar en <http://www.ibm.com/support/docview.wss?uid=swg21994390>.

**Nota:**

- Después de un escaneo incremental, los marcadores de resultados en el editor podrían dejar de encontrarse en la ubicación correcta.
- Resultados remediados que no tienen un rastreo pueden aparecer en resultados de escaneo incremental.
- No puede tener más de un producto o componentes de AppScan Source abiertos al mismo tiempo durante los escaneos incrementales. Además, otro usuario no puede escanear la misma aplicación o proyecto mientras usted mismo escanea, al mismo tiempo y en la misma máquina.

## Exclusión de un archivo de un escaneo

### Antes de empezar

**Nota:** Si la aplicación es un espacio de trabajo de Eclipse, no se pueden excluir archivos de los escaneos.

### Procedimiento

1. En la vista Explorador, seleccione el archivo o archivos que desea eliminar del escaneo.
2. Pulse con el botón derecho sobre la selección y elija **Excluir de escaneos** del menú.

### Resultados

Cuando se abre la vista Propiedades del proyecto que contiene el archivo, el separador **Orígenes** muestra una lista de archivos en el proyecto, incluidos los archivos excluidos.

Los archivos de proyecto se listan bajo el icono **Raíz de origen**. Los archivos que se excluyen del escaneo tienen un icono de archivo rojo (si se pulsa con el botón derecho del ratón sobre un archivo excluido, su menú tiene **Excluir** inhabilitado e

**Incluir** habilitado). Para excluir un archivo incluido, pulse con el botón derecho del ratón sobre dicho archivo y elija **Excluir** en el menú. Para incluir un archivo excluido, pulse con el botón derecho del ratón sobre dicho archivo y elija **Incluir** en el menú.

## Cancelar o detener un escaneo

Aunque puede cancelar un escaneo en curso, cancelarlo hace que se pierdan todos los datos relacionados con dicho escaneo. De forma alternativa, puede detener un escaneo para detener y producir un asesoramiento de los resultados encontrados hasta el momento.

### Cómo cancelar o detener un escaneo en AppScan Source for Analysis

Para cancelar un escaneo que está actualmente en curso, seleccione **Escanear > Cancelar escaneo** o **Escanear > Detener escaneo** en el menú principal.

**Cancelar escaneo** termina el escaneo y no produce ningún resultado. **Detener escaneo** detiene el escaneo y muestra los resultados encontrados hasta ahora.

### Cómo cancelar o detener un escaneo en AppScan Source for Development (plugin de Eclipse)

Mientras se está ejecutando el escaneo:

- Para cancelar el escaneo, elija **Análisis de seguridad > Escaneo > Cancelar escaneo** desde el menú principal. El escaneo termina y no produce ningún resultado; los mensajes de diagnóstico aparecen en la consola de Eclipse.
- Para detener el escaneo, elija **Análisis de seguridad > Escaneo > Detener escaneo** desde el menú principal. El escaneo termina y produce un asesoramiento de los resultados recopilados hasta el momento en que se ha iniciado la acción de detener.

**Nota:** Se da soporte a AppScan Source for Development (plugin de Eclipse) sólo en Windows y Linux.

### Cancelar un escaneo en AppScan Source for Development (plug-in de Microsoft Visual Studio)

Mientras se está ejecutando el escaneo, seleccione **IBM Security AppScan Source > Escanear > Cancelar escaneo** del menú principal. El escaneo termina y no produce ningún resultado.

**Nota:** Sólo se da soporte al plugin AppScan Source for Development Microsoft Visual Studio en Windows.

## Requisito previo de componentes de AppScan Source for Analysis y AppScan Source for Development (plugin de Eclipse) en Linux

En Linux, Eclipse requiere la instalación de un componente de terceros para poder mostrar contenido basado en navegador. Sin este componente, el plugin de AppScan Source for Analysis y AppScan Source for Development Eclipse puede mostrar síntomas como bloqueos después del inicio de sesión o un error durante la utilización del producto.

La información sobre este requisito previo está disponible en <http://www.eclipse.org/swt/faq.php#browserwebkitgtk>.

- “Habilitación de contenido basado en un navegador en Linux para AppScan Source for Analysis”
- “Habilitación de contenido basado en un navegador en Linux para AppScan Source for Development instalado en Eclipse Versión 3.7 o posterior”

## **Habilitación de contenido basado en un navegador en Linux para AppScan Source for Analysis**

AppScan Source for Analysis se basa en Eclipse y, por lo tanto, está afectado por este problema.

El enfoque recomendado para corregir esto es garantizar que esté instalada una versión de 32 bits o i686 de WebKitGTK 1.2.0 o posterior. Debe consultar al administrador del sistema cuál es la manera correcta de instalar paquetes, pero en algunos sistemas esto puede ser tan sencillo como emitir `yum install webkitgtk.i686`.

Si no puede instalar WebKitGTK, tiene la posibilidad de instalar una versión de 32 bits de Mozilla XULRunner 1.8. Con esta opción, puede que también necesite realizar estas actualizaciones en las variables de entorno:

- Establezca `MOZILLA_FIVE_HOME` en la ubicación de instalación XULRunner.
- Actualice `LD_LIBRARY_PATH` para incorporar (o añadir con anterioridad) `$MOZILLA_FIVE_HOME`

## **Habilitación de contenido basado en un navegador en Linux para AppScan Source for Development instalado en Eclipse Versión 3.7 o posterior**

El enfoque recomendado para corregir esto es garantizar que esté instalada una versión de 32 bits o i686 de WebKitGTK 1.2.0 o posterior. Debe consultar al administrador del sistema cuál es la manera correcta de instalar paquetes, pero en algunos sistemas esto puede ser tan sencillo como emitir `yum install webkitgtk.i686`.

Si no puede instalar WebKitGTK, tiene la posibilidad de instalar una versión de 32 bits de Mozilla XULRunner 1.8. Con esta opción, puede que también necesite realizar estas actualizaciones en las variables de entorno:

- Establezca `MOZILLA_FIVE_HOME` en la ubicación de instalación XULRunner.
- Actualice `LD_LIBRARY_PATH` para incorporar (o añadir con anterioridad) `$MOZILLA_FIVE_HOME`

---

## **Gestión de Mis asesoramientos**

La vista Mis asesoramientos contiene una lista de asesoramientos (el asesoramiento abierto actualmente, junto con otros asesoramientos que ha guardado). En esta vista, puede abrir, suprimir, guardar, renombrar o comparar asesoramientos. Cuando finaliza un escaneo o cuando el usuario abre un asesoramiento guardado, el asesoramiento aparece en la vista Mis asesoramientos. Mis asesoramientos muestra una tabla de asesoramientos abiertos o guardados e identifica un asesoramiento publicado o modificado. Si se elimina un asesoramiento de esta vista (sin guardarlo ni publicarlo se) suprime de forma permanente el asesoramiento.

Para obtener más información sobre la vista Mis asesoramientos, consulte “Vista Mis asesoramientos” en la página 313.

**Restricción:** Cuando realice un escaneo de varias aplicaciones o proyectos, se crea un nodo padre que contiene asesoramientos para cada elemento escaneado en la vista Mis asesoramientos. Los asesoramientos hijo individuales no se pueden gestionar en este caso (por ejemplo, los asesoramientos hijo no se pueden eliminar o publicar de forma individual). Cuando varias aplicaciones o proyectos se escanean a la vez, solo podrá gestionar los asesoramientos como un grupo (el nodo padre).

**Consejo:** Solo puede abrir los resultados de escaneo pertenecientes a una aplicación simultáneamente. Para ver los resultados de un escaneo de varias aplicaciones proyectos, debe ampliar el árbol en la vista Mis asesoramientos y realizar una doble pulsación sobre el asesoramiento que desea abrir.

---

## Envío de asesoramientos de AppScan Source a la nube para su análisis

Si posee una suscripción a IBM Application Security on Cloud en IBM Cloud Marketplace o a Application Security on Cloud for Bluemix, puede enviar asesoramientos de AppScan Source para su análisis a la nube. Se da soporte a los asesoramientos de AppScan Source versiones 9.0 o superiores. El número de escaneos que se pueden enviar dependen de su suscripción de Application Security on Cloud.

### Acerca de esta tarea

Cuando utiliza la característica de análisis estático del servicio de Application Security on Cloud, puede generar informes de análisis de seguridad que utilicen las analíticas de IFA (Intelligent Finding Analytics). IFA es una potente tecnología de aprendizaje de máquina que realiza automáticamente una gran parte del trabajo de selección, entre otras cosas, filtrando falsos positivos y agrupando los hallazgos que se pueden remediar con un arreglo en un punto de código. Para obtener más información sobre IFA, consulte este artículo.

Si está utilizando AppScan Source Versión 9.0 o superior y tiene una suscripción de Application Security on Cloud, puede aprovecharse de esta tecnología subiendo su asesoramiento de AppScan Source a Application Security on Cloud. A cambio, recibirá un nuevo asesoramiento que ha sido evaluado por esta tecnología. Este asesoramiento puede presentarse en forma de un informe HTML o abrirse en su producto de AppScan Source.

Si posee una suscripción de Application Security on Cloud, tiene un número limitado de escaneos por mes. Consulte [http://www.ibm.com/support/knowledgecenter/SSYJFF\\_1.0.0/ApplicationSecurityonCloud/src\\_managing\\_assessments\\_cloud.html](http://www.ibm.com/support/knowledgecenter/SSYJFF_1.0.0/ApplicationSecurityonCloud/src_managing_assessments_cloud.html) para obtener más información sobre los tipos de escaneos y escaneos simultáneos.

**Nota:** Si está escaneando un asesoramiento de AppScan Source con una prueba gratuita de Application Security on Cloud, puede descargar un informe HTML completo, además del archivo de asesoramiento de AppScan Source que IFA haya evaluado. Para todos los otros tipos de escaneo, sólo puede descargar un informe de resumen cuando tenga una prueba gratuita.

## Procedimiento

1. **Omita este paso si ya está utilizando Application Security on Cloud para análisis estático:**
  - a. Si no posee una suscripción de Application Security on Cloud, puede adquirir una tal como se indica a continuación:
    - **IBM Cloud Marketplace:** Vaya a <https://appscan.ibmcloud.com/serviceui/home> e inicie una sesión con su ID de IBM. Si no posee un ID de IBM, utilice el enlace para crear uno. A continuación inicie una sesión para una prueba gratuita o una suscripción de pago con los enlaces en el servicio.
    - **IBM Bluemix:** Vaya a <https://console.ng.bluemix.net/> y utilice el botón **SIGN UP** y complete el formulario para iniciar una sesión en Bluemix. A continuación, cree una instancia de servicio de Application Security on Cloud for Bluemix.
  - b. **Solo IBM Cloud Marketplace:** En el servicio Application Security on Cloud, cree una aplicación (consulte [http://www.ibm.com/support/knowledgecenter/SSYJFF\\_1.0.0/ApplicationSecurityonCloud/ent\\_create\\_application.html](http://www.ibm.com/support/knowledgecenter/SSYJFF_1.0.0/ApplicationSecurityonCloud/ent_create_application.html)) y, continuación, pulse **Crear escaneo**.
  - c. En la pantalla **¿Qué tipo de aplicación está escaneando hoy?**, seleccione **Escritorio** o **Web** > **Estática**.
  - d. Si de forma previa todavía no ha descargado ni configurado el Programa de utilidad de cliente de Static Analyzer, hágalo ahora. Consulte el apartado [http://www.ibm.com/support/knowledgecenter/SSYJFF\\_1.0.0/ApplicationSecurityonCloud/src\\_utility\\_install.html](http://www.ibm.com/support/knowledgecenter/SSYJFF_1.0.0/ApplicationSecurityonCloud/src_utility_install.html) para obtener más información.
2. Genere un asesoramiento (archivo .ozasmt) en la herramienta o producto de AppScan Source que elija. Se da soporte a la versión 9.0 y posteriores.
3. Utilice la interfaz de línea de mandatos (CLI) del programa de utilidad cliente para generar un archivo de Intermediate Representation (IRX o .irx) para el asesoramiento (.ozasmt):
  - a. Después de extraer el programa de utilidad cliente en una unidad local, añada la ubicación de su directorio \bin a su variable de entorno PATH. Si no lo hace, todos los mandatos de interfaz de línea de mandatos (CLI) de programa de utilidad cliente se deben calificar con el directorio \bin cada vez que los emita. Consulte el apartado [http://www.ibm.com/support/knowledgecenter/SSYJFF\\_1.0.0/ApplicationSecurityonCloud/src\\_irx\\_gen\\_cli.html](http://www.ibm.com/support/knowledgecenter/SSYJFF_1.0.0/ApplicationSecurityonCloud/src_irx_gen_cli.html) para obtener más información.
  - b. Emita este mandato en Windows:

```
appscan package -d <vía_acceso_guardar> -f <archivo_asesoramiento> -n <nombre_archivo>
```

o este mandato en Linux:

```
appscan.sh package -d <vía_acceso_guardar> -f <archivo_asesoramiento> -n <nombre_archivo>
```

Los argumentos del mandato son opcionales:
    - -d: especifique -d <vía\_acceso\_guardar>, donde <vía\_acceso\_guardar> es el directorio en el que desea guardar el archivo IRX.
    - -f: especifique -f <archivo\_asesoramiento>, donde <archivo\_asesoramiento> es el archivo .ozasmt que desea empaquetar para el escaneo. Si el archivo <archivo\_asesoramiento> no está en el directorio actual, utilice esta opción para especificar la vía de acceso y el nombre del archivo de asesoramiento.



**Nota:** Esta opción solo es necesaria si una o las dos sentencias siguientes son verdaderas:

- Emite el mandato desde un directorio que contiene más de un archivo de asesoramiento. Si el directorio solo contiene un archivo de asesoramiento, dicho archivo se empaquetará si no se utiliza la opción -f.
- Emite el mandato desde un directorio que no contiene archivos de asesoramiento. En este caso, se debe utilizar la opción -f para especificar la vía de acceso y el nombre del archivo de asesoramiento que se debe empaquetar.
- -n: Especifique -n <nombre\_archivo>, donde <nombre\_archivo> es el nombre de archivo de IRX. Puede especificar el nombre del archivo con o sin la extensión .irx. Si lo especifica sin la extensión, se añadirá automáticamente cuando se genere el archivo.

Encontrará información adicional sobre el mandato package, incluidos algunos ejemplos, en Mandatos de configuración (Windows) o Mandatos de configuración (Linux).

4. Utilice el mandato de interfaz de línea de mandatos (CLI) queue\_analysis para subir el archivo IRX.
  - a. Inicie una sesión en el servicio desde la interfaz de línea de mandatos (CLI). El método para hacerlo difiere en IBM Cloud Marketplace y IBM Bluemix. Encontrará información detallada sobre la autenticación en el servicio en la interfaz de línea de mandatos (CLI) en Mandatos de autenticación (Windows) o Mandatos de autenticación (Linux).

- **IBM Cloud Marketplace:**

Emita este mandato en Windows:

```
appscan scx_login -P <contraseña> -u <nombre_usuario> -persist
```

o este mandato en Linux:

```
appscan.sh scx_login -P <contraseña> -u <nombre_usuario> -persist
```

Se necesitan estos argumentos:

- -P: Especifique -P <contraseña>, donde <contraseña> es la contraseña que especificó al registrarse para el servicio Application Security on Cloud.
- -u: Especifique -u <nombre\_usuario>, donde <nombre\_usuario> es la dirección de correo electrónico que especificó al registrarse en el servicio Application Security on Cloud.

Este argumento es opcional:

- -persist: Intenta de nuevo la autenticación en el servicio de forma automática cuando caduca el archivo de señal.

- **IBM Bluemix:**

Emita este mandato en Windows:

```
appscan login -P <contraseña> -u <nombre_usuario> -persist
```

o este mandato en Linux:

```
appscan.sh login -P <contraseña> -u <nombre_usuario> -persist
```

Se necesitan estos argumentos:

- -P: especifique -P <contraseña>, donde <contraseña> es la contraseña indicada en las credenciales de servicio.
- -u: especifique -u <nombre\_usuario>, donde <nombre\_usuario> es el ID de enlace indicado en las credenciales de servicio.

Para determinar las credenciales de servicio de Bluemix, seleccione **Credenciales de servicio** en el panel de navegación izquierdo del Panel de control de servicio. Consulte Habilitar las aplicaciones externas para utilizar los servicios de Bluemix.

Este argumento es opcional:

- `-persist`: Intenta de nuevo la autenticación en el servicio de forma automática cuando caduca el archivo de señal.

b. Suba el archivo IRX con el mandato `queue_analysis`:

- Emita este mandato en Windows:

```
appscan queue_analysis -a <id_aplic> -f <irx_archivo>
-n <nombre_escaneo>
```

o este mandato en Linux:

```
appscan.sh queue_analysis -a <id_aplic> -f <irx_archivo>
-n <nombre_escaneo>
```

Se necesitan estos argumentos:

- `-f`: Especifique `-f <irx_archivo>`, donde `<irx_archivo>` es el archivo IRX que desea enviar para escanearlo. Si el archivo IRX no está en el directorio actual, utilice esta opción para especificar la vía de acceso del archivo IRX y el nombre de archivo.

**Nota:** Esta opción solo es necesaria si una o las dos sentencias siguientes son verdaderas:

- Emite el mandato desde un directorio que contiene más de un archivo IRX. Si el directorio solo contiene un archivo IRX, dicho archivo se enviará si no se utiliza la opción `-f`.
- Emite el mandato desde un directorio que no contiene archivos IRX. En este caso, la opción `-f` debe utilizarse para especificar la vía de acceso y el nombre del archivo IRX para enviarlo.
- `-n`: Especifique `-n <nombre_escaneo>`, donde `<nombre_escaneo>` es el nombre del escaneo que se realiza en la nube.
- `-a` (**solo IBM Cloud Marketplace**): Si está conectado al servicio Application Security on Cloud en IBM Cloud Marketplace, los archivos de IRX que se envíen a la nube deben estar asociados con una aplicación de Application Security on Cloud existente. Con esta opción, especifique `-a <id_aplic>`, donde `<id_aplic>` es el ID de la aplicación asociada. Para determinar el ID, utilice el mandato `list_apps`.
- Cuando se completa el mandato `queue_analysis`, se visualiza un ID para el trabajo de análisis. Si desea recibir el informe de análisis de Application Security on Cloud utilizando la interfaz de línea de mandatos (CLI), necesitará incluir este ID de trabajo en el mandato `get_result` - y anotarlo. Si utiliza la interfaz de línea de mandatos (CLI) para recibir el informe del análisis, tendrá la opción de recibirlo como un archivo de archivador (.zip) que incluirá un archivo .ozasmt para que el informe del análisis se pueda abrir en AppScan Source. Si únicamente está interesado en ver un informe HTML, utilice la interfaz de línea de mandatos (CLI) o el cliente web de Application Security on Cloud para descargar el informe.

Encontrará información más detallada sobre el mandato `queue_analysis` en Mandatos de análisis (Windows) o Mandatos de análisis (Linux).

5. Cuando se complete el análisis, recibirá un correo electrónico si subió el archivo IRX utilizando la interfaz de línea de mandatos (CLI) - o si seleccionó el

recuadro de selección **Enviarme un correo electrónico cuando se complete el escaneo** en el cliente web de Application Security on Cloud.

6. Elija un método para recuperar el informe del análisis. Puede utilizar la interfaz de línea de mandatos (CLI) `get_result` o utilizar el cliente web de Application Security on Cloud. Si utiliza la interfaz de línea de mandatos (CLI) para recibir el informe del análisis, tendrá la opción de recibirlo como un archivo de archivador (.zip) que incluirá un archivo .ozasmt para que el informe del análisis se pueda abrir en AppScan Source. Si únicamente está interesado en ver un informe HTML, utilice la interfaz de línea de mandatos (CLI) o el cliente web de Application Security on Cloud para descargar el informe.

**7. Complete este paso si desea utilizar el mandato `get_result` de la interfaz de línea de mandatos (CLI) para recuperar el informe del análisis:**

- a. Asegúrese de que desde la interfaz de línea de mandatos (CLI) ha iniciado una sesión en el servicio.

- b. Emita este mandato en Windows:

```
appscan get_result -d <vía_acceso_archivo> -i <id_trabajo> -t <tipo>
```

o este mandato en Linux:

```
appscan.sh get_result -d <vía_acceso_archivo> -i <id_trabajo> -t <tipo>
```

Se necesite este argumento:

- `-i`: especifique `-i <id_trabajo>`, donde `<id_trabajo>` es el ID del trabajo de análisis.

**Nota:** Si no anotó el ID al emitir el mandato `queue_analysis`, utilice el mandato `appscan list` o `appscan.sh list` para ver una lista de todos los trabajos de análisis. Consulte Mandatos de análisis (Windows) o Mandatos de análisis (Linux) para obtener más información.

Estos argumentos son opcionales:

- `-d`: Especifique `-d <vía_acceso_archivo>`, donde `<vía_acceso_archivo>` es la vía de acceso completa del archivo de destino y/o el nombre del archivo de destino. Si no se especifica ningún nombre de archivo, el nombre de archivo se basará en el nombre del trabajo de escaneo. Si no se especifica ninguna vía de acceso, el archivo se guardará en el directorio actual. Si no se incluye esta opción, el archivo se guardará en el directorio actual con un nombre que se base en el nombre del trabajo de escaneo.
- `-t`: Especifique `-t <tipo>`, donde `<tipo>` es `html` o `zip`. Los resultados se guardarán como un archivo HTML o como un archivo .zip que contenga los resultados HTML. Si esta opción no se incluye, los resultados se guardarán como un archivo HTML.

Si los resultados del escaneo corresponden a un archivo IRX generado mediante el mandato `package`, si especifica `-t zip` se guardarán los resultados que contengan un nuevo archivo .ozasmt que se pueda cargar en el producto AppScan Source Versión 9.0 o posterior.

Encontrará información más detallada sobre el mandato `get_result` en Mandatos de resultados (Windows) o Mandatos de resultados (Linux).

8. **Complete este paso si desea utilizar el cliente web para recuperar el informe del análisis:** Si está únicamente interesado en visualizar un informe HTML, utilice el cliente web de Application Security on Cloud para descargar el informe.

Cuando inicia una sesión en el servicio, debería ver de forma automática una lista de escaneos (si ha navegado a otra sección del servicio, pulse el icono X en

la parte superior derecha para volver a la lista de escaneos). En la lista de escaneos, ubique el escaneo y seleccione el icono **Descargar** y, a continuación, elija el formato XML o HTML.

Para aprender más sobre los resultados de escaneo de Application Security on Cloud en IBM Cloud Marketplace, consulte [http://www.ibm.com/support/knowledgecenter/en/SSYJFF\\_1.0.0/ApplicationSecurityonCloud/appseccloud\\_results\\_dashboard\\_cm.html](http://www.ibm.com/support/knowledgecenter/en/SSYJFF_1.0.0/ApplicationSecurityonCloud/appseccloud_results_dashboard_cm.html). En IBM Bluemix, consulte [https://console.ng.bluemix.net/docs/services/ApplicationSecurityonCloud/appseccloud\\_results.html#results](https://console.ng.bluemix.net/docs/services/ApplicationSecurityonCloud/appseccloud_results.html#results).

---

## Publicación de asesoramientos

AppScan Source ofrece dos opciones de publicación. Con la finalidad de guardar y compartir los asesoramientos, puede publicarlos en la base de datos de AppScan Source. O bien, si AppScan Enterprise Server se ha instalado con la opción Enterprise Console, podrá publicar asesoramientos en ella. AppScan Enterprise Console ofrece una variedad de herramientas para trabajar con asesoramientos, como características de informes, gestión de problemas, análisis de tendencias y paneles de control.

Para obtener más información sobre las funciones de publicación de AppScan Source, consulte los apartados “Publicación de asesoramientos en AppScan Source” en la página 133 y “Publicación de asesoramientos en AppScan Enterprise Console” en la página 135.

**Nota:** Con algunas versiones de AppScan Source y AppScan Enterprise, el nivel del release y la versión de los dos productos deben coincidir con el propósito de publicar desde AppScan Source en AppScan Enterprise Console. Consulte <http://www.ibm.com/support/docview.wss?uid=swg21975211> para saber qué versiones de AppScan Source y AppScan Enterprise son compatibles al publicar asesoramientos.

## Registro de aplicaciones y proyectos para publicar en AppScan Source

Para poder publicar un asesoramiento en la base de datos de base de datos de AppScan Source, antes debe registrar las aplicaciones o los proyectos que se han escaneado para crearlo. De forma predeterminada, si intenta publicar un asesoramiento de aplicaciones o proyectos que no están registrados, se le solicitará que registre las aplicaciones o los proyectos en ese momento. AppScan Source for Analysis *registra automáticamente* por usted si su preferencia **General, Aplicaciones registradas automáticamente en una publicación inicial**, es **Registrar siempre**.

**Importante:** Debe tener permiso **Registrar** para poder registrar aplicaciones y proyectos.

Para registrar las aplicaciones y proyectos antes de escanearlos, seleccione las aplicaciones o proyectos en la vista Explorador y seleccione **Archivo > Registrar** en el menú principal del espacio de trabajo. Las acciones **Registrar aplicación** y **Registrar proyecto** también están disponibles si pulsa con el botón derecho los elementos seleccionados en la vista Explorador.

Si una aplicación ya está registrada, puede volverla a registrar con un nuevo nombre. Para ello, seleccione y pulse con el botón derecho y luego elija **Registrar aplicación como** en el menú. En el cuadro de diálogo Renombrar, escriba un nuevo nombre para la aplicación o proyecto registrado.

Para anular el registro de aplicaciones y proyectos, seleccione las aplicaciones o proyectos en la vista Explorador y luego seleccione **Archivo > Anular registro** en el menú principal del espacio de trabajo. Las acciones **Aplicación sin registrar** y **Proyecto sin registrar** también están disponibles cuando pulsa con el botón derecho en los elementos seleccionados en la vista Explorador.

**Nota:** Al anular el registro de un elemento no se eliminan los datos publicados desde el servidor de AppScan Source.

## Publicación de asesoramientos en AppScan Source

Con la finalidad de guardar y compartir los asesoramientos, puede publicarlos en la base de datos de AppScan Source.

### Acerca de esta tarea

Las aplicaciones y los proyectos deben registrarse primero en AppScan Source para que se puedan publicar los asesoramientos. Consulte el apartado “Registro de aplicaciones y proyectos para publicar en AppScan Source” en la página 132 para obtener más información. De forma predeterminada, si intenta publicar un asesoramiento de aplicaciones o proyectos que no están registrados, se le solicitará que registre las aplicaciones o los proyectos en ese momento (lo que necesita el permiso **Registrar**).

**Nota:** Los asesoramientos creados como resultado del escaneo de archivos individuales no se pueden publicar.

**Restricción:** Cuando realice un escaneo de varias aplicaciones o proyectos, se crea un nodo padre que contiene asesoramientos para cada elemento escaneado en la vista Mis asesoramientos. Los asesoramientos hijo individuales no se pueden gestionar en este caso (por ejemplo, los asesoramientos hijo no se pueden eliminar o publicar de forma individual). Cuando varias aplicaciones o proyectos se escanean a la vez, solo podrá gestionar los asesoramientos como un grupo (el nodo padre).

### Procedimiento

1. Para publicar el asesoramiento que esté abierto actualmente en la perspectiva Selección, en el menú principal del espacio de trabajo seleccione **Archivo > Publicar asesoramiento en AppScan Source**.
2. Para publicar un asesoramiento en la vista Mis asesoramientos, selecciónelo y pulse el botón **Publicar asesoramiento en AppScan Source** en la vista, o bien pulse con el botón derecho en el asesoramiento y seleccione **Publicar asesoramiento en AppScan Source**.

### Resultados

Cuando guarda un asesoramiento, AppScan Source for Analysis graba vías de acceso absolutas en el archivo de asesoramiento para hacer referencia a elementos como archivos de origen. Estas vías de acceso absolutas puede dificultar la compartición del archivo en otro sistema que tiene distintas estructuras de directorios. Para poder crear archivos de asesoramiento portátiles, debe crear una variable (consulte el apartado “Definición de variables” en la página 99 o “Definición de variables cuando se publican y se guardan” en la página 142).

Una vez publicado, el asesoramiento que se lista en la vista Mis asesoramientos contará con un icono en la columna **Publicado**. Además, el asesoramiento

aparecerá en la vista Asesoramientos publicados, que es una vista controlada por filtros de los asesoramientos publicados en la base de datos de AppScan Source. Se puede definir la vista para que sólo muestre los asesoramientos que coinciden con los criterios de filtro. Por ejemplo, si se publican 1.000 asesoramientos, y solo desea ver los asesoramientos que ha publicado, puede crear un filtro **Por aplicación de publicación** como criterio y **Usuario actual** o su nombre de usuario como valor.

### Definición de un filtro en la vista Asesoramientos publicados

Se pueden utilizar filtros para limitar el número de asesoramientos que se visualizan en la vista Asesoramientos publicados.

#### Procedimiento

1. En la vista Asesoramientos publicados, pulse el botón **Establecer filtro** de la barra de herramientas.
2. Marque el cuadro (o los cuadros) de selección de los criterios de filtro que desee:
  - **Por aplicación:** seleccione la aplicación para la cual desea que se muestren los asesoramientos. Los asesoramientos que se han generado para varias aplicaciones aparecerán si la aplicación especificada formaba parte del asesoramiento.
  - **Por aplicación de publicación:** establece la vista para ver los asesoramientos que ha publicado el usuario actual, o bien permite especificar el usuario cuyos asesoramientos publicados desea ver.
  - **Por fecha de proximidad:** especifique un rango de fechas con relación a la fecha actual en horas, días, semanas, meses o años. Puede seleccionar **Por fecha de proximidad** o **Por rango de fecha**, pero no ambos.
  - **Por rango de fecha:** especifique un rango de fechas del asesoramiento que se mostrará en la vista. Puede seleccionar **Por fecha de proximidad** o **Por rango de fecha**, pero no ambos.
3. Pulse **Aceptar** para establecer el filtro.

#### Resultados

Pulse **Renovar filtro** tras aplicar los criterios de filtro para renovar la vista con los asesoramientos añadidos o eliminados desde que se aplicó el filtro por última vez. Pulse **Borrar filtro** para eliminar un filtro existente y que se muestren todos los asesoramientos.

### Supresión de asesoramientos publicados de AppScan Source

Si ha publicado un asesoramiento en AppScan Source, puede utilizar acciones en la vista Asesoramientos publicados para eliminarlos.

#### Procedimiento

1. En la vista Asesoramientos publicados, seleccione el asesoramiento que desee suprimir. También se puede seleccionar varios asesoramientos utilizando las teclas Control o Mayúsculas del teclado.
2. Seleccione el botón **Suprimir asesoramientos** en la barra de herramientas de la vista, o pulse con el botón derecho del ratón sobre la selección y seleccione **Suprimir asesoramientos** en el menú.

## Publicación de asesoramientos en AppScan Enterprise Console

Si AppScan Enterprise Server se ha instalado con la opción Enterprise Console, podrá publicar asesoramientos en ella. Enterprise Console ofrece una variedad de herramientas para trabajar con asesoramientos, como características de informes, gestión de problemas, análisis de tendencias y paneles de control.

### Acerca de esta tarea

Para poder publicar asesoramientos en Enterprise Console, primero debe configurar los valores del servidor en la página de preferencias de AppScan Enterprise Console. Para obtener información sobre cómo definir preferencias, consulte “Preferencias de AppScan Enterprise Console” en la página 96.

**Nota:** Con algunas versiones de AppScan Source y AppScan Enterprise, el nivel del release y la versión de los dos productos deben coincidir con el propósito de publicar desde AppScan Source en AppScan Enterprise Console. Consulte <http://www.ibm.com/support/docview.wss?uid=swg21975211> para saber qué versiones de AppScan Source y AppScan Enterprise son compatibles al publicar asesoramientos.

**Restricción:** Cuando realice un escaneo de varias aplicaciones o proyectos, se crea un nodo padre que contiene asesoramientos para cada elemento escaneado en la vista Mis asesoramientos. Los asesoramientos hijo individuales no se pueden gestionar en este caso (por ejemplo, los asesoramientos hijo no se pueden eliminar o publicar de forma individual). Cuando varias aplicaciones o proyectos se escanean a la vez, solo podrá gestionar los asesoramientos como un grupo (el nodo padre).

### Procedimiento

1. Utilice uno de estos métodos para publicar uno o varios asesoramientos en Enterprise Console:
  - a. Seleccione uno o varios asesoramientos en la vista Mis asesoramientos y pulse **Publicar asesoramiento en AppScan Enterprise Console**.
  - b. Pulse con el botón derecho en el asesoramiento (o en una selección de asesoramientos) en la vista Mis asesoramientos y seleccione el elemento de menú **Publicar asesoramiento en AppScan Enterprise Console**.
  - c. Cuando se abra un asesoramiento, elija **Archivo > Publicar asesoramiento en AppScan Enterprise Console** en el menú principal.
2. En el recuadro de diálogo Publicar en AppScan Enterprise Console:
  - a. Especifique una aplicación de AppScan Enterprise Console para asociarla con el asesoramiento. Esto es necesario al conectarse a AppScan Enterprise Server Versión 9.0.3 y superior (a no ser que inhabilite el requisito, tal como se describe aquí). La asociación con una aplicación es opcional al conectarse a versiones anteriores de AppScan Enterprise Server. Si está conectado a una versión anterior de AppScan Enterprise Server, de forma predeterminada, la aplicación se establece en la última aplicación que se especificó para ser publicada. Si no se especificaron con anterioridad aplicaciones al publicar, no habrá un valor predeterminado. Para especificar una aplicación:
    - 1) Pulse el campo **Aplicación** botón **Seleccionar**.

- 2) Se abre el recuadro de diálogo Seleccionar aplicación, visualizando todas las aplicaciones que ya existen en AppScan Enterprise Console. Si desea ver los atributos de una aplicación en AppScan Enterprise Console, pulse **Ver perfil** junto a la misma.
- 3) Seleccione la aplicación para asociarla al escaneo, o cree una nueva aplicación con este propósito pulsando **Crear nueva aplicación**. Al pulsar este enlace se abre AppScan Enterprise Console donde puede crear una nueva aplicación. Una vez se hayan guardado los atributos de la nueva aplicación, el recuadro de diálogo Seleccionar aplicación se renovará de forma automática para incluir la selección (si la nueva aplicación no se incluye de forma automática, pulse **Renovar**).

**Consejo:** En el recuadro de diálogo Seleccionar aplicación, se puede utilizar el campo de filtro para acotar la lista de aplicaciones. A medida que escribe, el filtro se aplica automáticamente a la lista de aplicaciones. Los caracteres asterisco (\*) y signo de interrogación (?) se pueden utilizar como caracteres comodín. Un asterisco coincide con cualquier grupo de cero o más caracteres, mientras que una interrogación coincide con un carácter único.

- 4) Pulse **Aceptar** una vez haya seleccionado la aplicación.
- b. Necesario: En el campo **Nombre**, especifique un nombre con el que se guardará el asesoramiento en AppScan Enterprise Console.
- c. Opcional: **Cuando se conecta a versiones de AppScan Enterprise Server anteriores a la versión 9.0.3:** Utilice el campo **Carpeta** para establecer la ubicación en la que publicar. De forma predeterminada, la ubicación se establece en la última ubicación que se ha utilizado para la publicación. Si no se ha publicado anteriormente ningún asesoramiento, se selecciona la carpeta de AppScan Enterprise Console predeterminada (tenga en cuenta que es la carpeta predeterminada del ID de usuario que se ha especificado en la página de preferencias de AppScan Enterprise Console). Para elegir una carpeta distinta en la que publicar, pulse el campo **Carpeta** botón **Seleccionar** y, a continuación, elija la carpeta que desee (únicamente estarán disponibles las carpetas en las que tenga permiso para publicar). Si la carpeta donde desea publicar no está disponible, pulse **Renovar** para actualizar el árbol de carpeta con los cambios que se hayan realizado en el servidor.

3. Pulse **Publicar**.

## Resultados

Cuando guarda un asesoramiento, AppScan Source for Analysis graba vías de acceso absolutas en el archivo de asesoramiento para hacer referencia a elementos como archivos de origen. Estas vías de acceso absolutas puede dificultar la compartición del archivo en otro sistema que tiene distintas estructuras de directorios. Para poder crear archivos de asesoramiento portátiles, debe crear una variable (consulte el apartado “Definición de variables” en la página 99 o “Definición de variables cuando se publican y se guardan” en la página 142).

Una vez publicado el asesoramiento, se proporcionará un enlace con AppScan Enterprise (Enterprise Console) en un mensaje informativo. Cuando se pulse en el enlace, se abrirá la página del portal con el navegador web externo predeterminado.

**Consejo:** Si la publicación falla, compruebe que el servidor de Enterprise Console se esté ejecutando y que pueda acceder a su URL de centro de control en un



navegador (utilice la misma **URL de Enterprise Console** que ha especificado en la página de preferencias de AppScan Enterprise Console).

**Nota:**

- Los asesoramientos grandes tardan más en aparecer en el portal. Si no recibe ningún mensaje de error después de la publicación y el informe no aparece en el portal, póngase en contacto con el administrador.
- Si intenta publicar un asesoramiento que tenga el mismo nombre que uno que Enterprise Console esté procesando actualmente, se producirá un error. Además, si publica el asesoramiento con el nombre común después de que se haya procesado el primero, el segundo asesoramiento sobregrabará el primero (Enterprise Console puede ofrecer un análisis de tendencia para informes con nombres comunes si se ha configurado previamente para que lo haga). Para determinar si un asesoramiento se ha terminado de procesar, acceda al centro de control de Enterprise Console en un navegador web y vaya a la carpeta de usuario adecuada y compruebe el estado del informe.
- AppScan Source no da soporte a la publicación en una instancia de Enterprise Console que se haya configurado para utilizar valores de proxy. Si se intenta publicar en una instancia que utiliza valores de proxy, se producirá un error.

**Importante:**

Cuando se actualiza a AppScan Source Versión 9.0.3.4, observará estos cambios:

- Cuando publique un asesoramiento en AppScan Enterprise Console, ahora deberá asociar el asesoramiento con una aplicación en AppScan Enterprise (si está ejecutando AppScan Enterprise Server Versión 9.0.3 y superior). Como resultado, los scripts de automatización podrían fallar si no incluyen la asociación con la aplicación. En AppScan Enterprise Server, se necesita la asociación de la aplicación si desea sacar partido de las características de gestión de riesgos de seguridad de aplicaciones de AppScan Enterprise Server. Consulte [http://www.ibm.com/support/knowledgecenter/SSW2NF\\_9.0.3/com.ibm.ase.help.doc/topics/c\\_overview.html](http://www.ibm.com/support/knowledgecenter/SSW2NF_9.0.3/com.ibm.ase.help.doc/topics/c_overview.html).
- Además, debe eliminar el puerto del URL de AppScan Enterprise.
  1. En AppScan Source for Analysis, pulse **Editar > Preferencias**.
  2. En los valores de la consola de AppScan Enterprise, elimine el puerto del campo **URL de Enterprise Console**.
- Después de publicar su asesoramiento, únicamente estará disponible en la vista de supervisor de AppScan Enterprise (en releases anteriores, los asesoramientos estaban disponibles en la vista de escaneos de AppScan Enterprise). La migración a esta vista se describe en [http://www.ibm.com/support/knowledgecenter/SSW2NF\\_9.0.3/com.ibm.ase.help.doc/topics/t\\_workflow\\_for\\_applications.html](http://www.ibm.com/support/knowledgecenter/SSW2NF_9.0.3/com.ibm.ase.help.doc/topics/t_workflow_for_applications.html).

Esto se debe a un cambio en el protocolo de comunicación entre AppScan Source y AppScan Enterprise Server, que es necesario para publicar en AppScan Enterprise Server cuando se utiliza la autenticación con CAC (Common Access Card).

Si no desea publicar asesoramientos en AppScan Enterprise Server cuando la autenticación con CAC está habilitada, o si no desea aprovechar las características de gestión de riesgos de seguridad de aplicaciones de Enterprise Server, puede volver al protocolo de comunicación anterior de la siguiente manera:

1. Abra <dir\_datos>\config\ounce.ozsettings (donde <data\_dir> es la ubicación de los datos de programa AppScan Source, como se describe en “Instalación y ubicaciones de archivo de datos de usuario” en la página 335)).

2. En este archivo, localice este valor:

```
<Setting
  name="force_ase902_assessment_publish"
  value="false"
  default_value="false"
  description="Use ASE 9.0.2-style assessment publish"
  display_name="Use ASE 9.0.2-style assessment publish"
  type="boolean"
  read_only="true"
  hidden="true"
/>
```

3. En el valor, cambie value="false" por value="true" y, a continuación, guarde el archivo.
4. Reinicie el producto de AppScan Source desde el que publicará los asesoramientos.

Cuando este valor se establece en value="true":

- Si asocia un asesoramiento con una aplicación en AppScan Enterprise al realizar la publicación, el asesoramiento estará disponible en las vistas de supervisión y escaneos.
- Si no asocia un asesoramiento con una aplicación, al realizar la publicación, el asesoramiento estará disponible en la vista de escaneos.
- No podrá publicar asesoramientos en AppScan Enterprise Server cuando la autenticación con CAC esté habilitada.

Para obtener más información, consulte <http://www.ibm.com/support/docview.wss?uid=swg21993010>.

## Preferencias de AppScan Enterprise Console

Si AppScan Enterprise Server se ha instalado con la opción AppScan Enterprise Console, puede publicar asesoramientos en la misma. Enterprise Console ofrece una variedad de herramientas para trabajar con asesoramientos, como característica de informes, gestión de problemas, análisis de tendencias y paneles de control.

Para habilitar esta función, complete la página de preferencias de AppScan Enterprise Console. Todos los campos de esta página deben completarse con entradas válidas para que se habilite la publicación de Enterprise Console:

- **Campo ID de usuario:** Especifique su ID de usuario de AppScan Enterprise Server (el ID de usuario que se creó para la publicación en representación de su usuario de AppScan Source).
  - Si se ha configurado AppScan Enterprise Server para utilizar la autenticación de Windows, escriba el dominio y el nombre de usuario que utiliza para conectarse con Enterprise Console (separe el dominio y el nombre de usuario con una barra invertida, \, por ejemplo, mi\_dominio\mi\_nombreusuario).
  - Si se ha configurado AppScan Enterprise Server con LDAP, escriba el nombre de usuario que ha utilizado para conectarse con Enterprise Console.
  - En Windows, si AppScan Enterprise Server está habilitado para la autenticación CAC (Common Access Card), seleccione su Nombre común CAC de la lista.

Como mínimo, debe ser un usuario de QuickScan. Si está conectado a una instancia de AppScan Enterprise Server anterior a la versión 9.0.3, debe tener su propia carpeta en Enterprise Server.

- **Campo Contraseña:** Este campo únicamente está disponible si su método de autenticación de AppScan Enterprise Server es mediante ID de usuario y

contraseña. Especifique la contraseña que se ha utilizado para iniciar sesión en Enterprise Console (la contraseña para el nombre de usuario que se ha entrado).

- **Campo URL de Enterprise Console:** Especifique el URL utilizado para acceder a la aplicación web de Enterprise Console.

El formato de esta URL es:

`http(s)://<nombrehost>:<puerto>/ase`

Donde <nombrehost> es el nombre de la máquina en la que se ha instalado Enterprise Console y <puerto> es el puerto en el que la consola está en ejecución (el <puerto> predeterminado es 9443). Un ejemplo de URL es `https://myhost.mydomain.ibm.com:9443/ase`.

**Nota:**

- Este campo no se ha de modificar si ya se ha definido **URL de Enterprise Console**.
- Debe haber iniciado la sesión en AppScan Source con permiso para **Gestionar configuraciones de AppScan Enterprise** para poder definir el campo **URL de Enterprise Console**. Para obtener información sobre cuentas y permisos de usuarios, consulte la sección sobre *Administración* del InfoCenter del producto o la sección *Administración de AppScan Source* de la publicación *IBM Security AppScan Source Guía de instalación y administración*.
- El **ID de usuario** y la **Contraseña** se guardan en la máquina que ejecuta el cliente de AppScan Source (por ejemplo, AppScan Source for Analysis) - mientras que **URL de Enterprise Console** se guarda en Enterprise Server (que puede estar ubicado en una máquina remota). No puede acceder a la información del nombre de usuario y contraseña desde la máquina remota (por ejemplo, utilizando el mandato `getaseinfo` desde la misma).
- AppScan Source no da soporte a la publicación en una instancia de AppScan Enterprise Console que se haya configurado para utilizar valores de proxy. Si se intenta publicar en una instancia que utiliza valores de proxy, se producirá un error.

Tras completar los valores, se recomienda encarecidamente asegurarse de que la conexión con el servidor de Enterprise Console sea válida pulsando **Probar conexión**.

**Consejo:** Si la prueba de conexión falla, compruebe que el servidor de Enterprise Console se esté ejecutando y que pueda acceder a su URL de centro de control en un navegador (utilice el mismo valor de **URL de Enterprise Console** que ha especificado anteriormente).

---

## Guardar asesoramientos

### Antes de empezar

**Importante:** Para guardar asesoramientos, debe tener el permiso **Guardar asesoramientos**. Para obtener información sobre cómo establecer permisos, consulte el manual *IBM Security AppScan Source Guía de instalación y administración*.

### Acerca de esta tarea

Los asesoramientos se pueden guardar localmente y volver abrirlos posteriormente cualquier momento. De forma predeterminada, los asesoramientos se guardan con una extensión de archivo `.ozasmt` en el directorio de inicio del sistema operativo

(por ejemplo, en Windows, el directorio puede ser C:\Documents and Settings\Administrator\).

## Procedimiento

1. Para guardar el asesoramiento abierto actualmente en la perspectiva Selección, seleccione **Archivo > Guardar asesoramiento** o **Archivo > Guardar asesoramiento como** en el menú principal del entorno de trabajo. Si elige la acción **Guardar asesoramiento como** puede especificar la ubicación y el nombre de archivo del asesoramiento guardado.
2. Para guardar un asesoramiento en la vista Mis asesoramientos, selecciónelo y pulse el botón de la vista **Guardar asesoramiento** o **Guardar asesoramiento como**, o bien pulse el asesoramiento con el botón derecho y seleccione **Guardar asesoramiento** o **Guardar asesoramiento como**.

## Resultados

Cuando guarda un asesoramiento, AppScan Source for Analysis graba vías de acceso absolutas en el archivo de asesoramiento para hacer referencia a elementos como archivos de origen. Estas vías de acceso absolutas puede dificultar la compartición del archivo en otro sistema que tiene distintas estructuras de directorios. Para poder crear archivos de asesoramiento portátiles, debe crear una variable (consulte el apartado “Definición de variables” en la página 99 o “Definición de variables cuando se publican y se guardan” en la página 142).

## Guardar asesoramientos automáticamente

De forma predeterminada, los escaneos se guardan automáticamente en `<data_dir>\scans` (donde `<data_dir>` es la ubicación de los datos de programa AppScan Source, como se describe en “Instalación y ubicaciones de archivo de datos de usuario” en la página 335) durante un periodo de tres días. Este comportamiento está determinado por los valores `assessment_auto_save`, `assessment_auto_save_location` y `assessment_auto_save_stale_period` en `<data_dir>\config\scanner.ozsettings`.

- Si el valor `assessment_auto_save` está establecido en `true`, los asesoramientos se guardan automáticamente cuando se completan (debe tener permiso de **Guardar asesoramientos**).
- El valor `assessment_auto_save_location` determina la ubicación en la que se almacenan los asesoramientos. De forma predeterminada, asesoramientos se guardan en `<data_dir>\scans`. Para cambiar esta ubicación, establezca el atributo `value` en el directorio que desee. Por ejemplo, para establecer la ubicación en `C:\myFolder`, establezca el atributo en `value="C:\myFolder"`.
- El valor `assessment_auto_save_stale_period` determina el número de días que se guardarán los asesoramientos en `assessment_auto_save_location`. Puede alterar este valor con el atributo `value`. Por ejemplo, los asesoramientos guardados se eliminarán de `assessment_auto_save_location` después de 10 días si el atributo se establece en `value="10"`.

---

## Eliminación de asesoramientos de Mis asesoramientos

Al eliminar asesoramientos de la vista Mis asesoramientos, no se eliminan de su sistema local. Si se elimina un asesoramiento de la vista, se puede volver a añadir con la acción **Abrir asesoramiento**.

## Acerca de esta tarea

**Restricción:** Cuando realice un escaneo de varias aplicaciones o proyectos, se crea un nodo padre que contiene asesoramientos para cada elemento escaneado en la vista Mis asesoramientos. Los asesoramientos hijo individuales no se pueden gestionar en este caso (por ejemplo, los asesoramientos hijo no se pueden eliminar o publicar de forma individual). Cuando varias aplicaciones o proyectos se escanean a la vez, solo podrá gestionar los asesoramientos como un grupo (el nodo padre).

## Procedimiento

1. En la vista Mis asesoramientos, seleccione el asesoramiento que desee eliminar. También se puede seleccionar varios asesoramientos utilizando las teclas Control o Mayúsculas del teclado.
2. Seleccione el botón **Eliminar de Mis asesoramientos** en la barra de herramientas de la vista, o pulse con el botón derecho del ratón sobre la selección y seleccione **Eliminar de Mis asesoramientos** en el menú.

---

## Definición de variables

Cuando guarda asesoramientos o paquetes, o cuando publica asesoramientos, es posible que AppScan Source for Analysis le sugiera que cree una variable para sustituir las vías de acceso absolutas (sin variables, AppScan Source for Analysis graba las vías de acceso absolutas en el archivo de asesoramiento para hacer referencia a elementos, tales como los archivos de origen). Cuando configura variables para vías de acceso absolutas, facilita que se compartan los asesoramientos en varios sistemas. Cuando se comparten asesoramientos, se recomienda utilizar variables.

## Acerca de esta tarea

Las variables se pueden crear antes de iniciar una acción de guardar o publicar siguiendo las instrucciones de este tema, o bien se pueden crear después de iniciar la acción de guardar o publicar siguiendo los pasos del tema “Definición de variables cuando se publican y se guardan” en la página 142.

Por ejemplo, para obtener información acerca de cómo las variables pueden servir de ayuda cuando se comparten asesoramientos, consulte la sección “Ejemplo: definición de variables” en la página 142.

## Procedimiento

1. En el menú principal, seleccione **Ventana > Preferencias**. En el cuadro de diálogo Preferencias, seleccione **Cambiar variables**.
2. Pulse el botón **Añadir variable** en la página de preferencias Cambiar variables.
3. Entre un nombre para la variable y vaya a la ubicación del archivo, que será sustituido por la variable (AppScan Source for Analysis inserta los símbolos de porcentaje (%) al inicio y fin después de que se crea la variable).
4. Repita el paso anterior para cualquier otro elemento de referencia del asesoramiento (por ejemplo, si el asesoramiento hace referencia al origen en varias ubicaciones, añada una variable para cada ubicación).
5. Utilice la página de preferencias para editar y eliminar variables, mediante los botones **Modificar variable** y **Suprimir variable**.
6. Pulse **Aceptar** cuando haya acabado de definir las variables.

## Definición de variables cuando se publican y se guardan

Cuando intenta guardar o publicar un asesoramiento, AppScan Source for Analysis detecta las vías de acceso absolutas en el asesoramiento. Si no se han creado las variables correspondientes para las vías de acceso absolutas, se le solicitará que las cree.

### Acerca de esta tarea

Las variables se pueden crear antes de iniciar una acción de guardar o publicar siguiendo las instrucciones de “Definición de variables” en la página 99, o bien se pueden crear después de iniciar la acción de guardar o publicar siguiendo los pasos de este tema.

Por ejemplo, para obtener información acerca de cómo las variables pueden servir de ayuda cuando se comparten asesoramientos, consulte la sección “Ejemplo: definición de variables”.

### Procedimiento

1. Después de iniciar la acción de guardar o publicar, pulse **Sí** en el mensaje Se han detectado vías de acceso absolutas.
2. En el cuadro de diálogo Definir variables, AppScan Source for Analysis sugiere un conjunto de vías de acceso que abarcan los datos.
3. Seleccione un directorio y pulse **Añadir variable**.
4. Repita el paso anterior para cualquier otro elemento de referencia del asesoramiento (por ejemplo, si el asesoramiento hace referencia al origen en varias ubicaciones, añada una variable para cada ubicación).
5. El recuadro de diálogo Definir variables también puede utilizarse para editar y eliminar variables, mediante los botones **Modificar variable** y **Suprimir variable**.
6. Pulse **Aceptar** para completar la acción de guardar o publicar.

## Ejemplo: definición de variables

Para compartir datos de asesoramiento, debe definir las variables adecuadas. El ejemplo de este tema muestra la necesidad de una variable.

El usuario Joe realiza un escaneo en el sistema A, donde todo el código fuente se encuentra bajo el directorio C:\dev\my\_code. Joe desea guardar los resultados de su escaneo en un archivo y compartirlo con Bill. Bill utiliza el sistema B y tiene el mismo código que Joe ha escaneado bajo el directorio C:\code\bill's\_code. Sin variables, el archivo de asesoramiento hará referencia a todos los archivos fuente con vías de acceso que comenzarán por C:\dev\my\_code. Si Bill abre el archivo de asesoramiento en el sistema B, AppScan Source for Analysis no encontrará los archivos fuente, ya que se encuentran bajo C:\code\bill's\_code en el sistema B.

### Solución

Tanto Joe como Bill deben crear una variable que apunte a la raíz del código fuente. Joe crea una variable en AppScan Source for Analysis llamada SRC\_ROOT y le asigna el valor C:\dev\my\_code. Esta variable es local de la instalación de AppScan Source for Analysis de Joe. A continuación, Joe comunica a Bill el nombre de la variable (SRC\_ROOT) y la ubicación a la que apunta. Luego Bill crea una variable llamada SRC\_ROOT con el valor C:\code\bill's\_code, en su instalación de AppScan Source for Analysis. Cuando Joe guarda su escaneo, la variable SRC\_ROOT

sustituye la vía de acceso `C:\dev\my_code`. Cuando Bill abre el archivo de asesoramiento que ha recibido de Joe, `C:\code\bill's_code` sustituye la variable `SRC_ROOT`.





---

## Capítulo 5. Selección y análisis

La agrupación de resultados similares permite a los analistas de seguridad y a los auditores de IT segmentar y seleccionar problemas del código fuente. En esta sección se explica cómo seleccionar asesoramientos de AppScan Source y analizar resultados.

Cuando escanea código, aparecen los *resultados* del escaneo. *Selección* es el proceso de evaluar los resultados y determinar cómo resolverlos. Sin embargo, los pasos a seguir para alcanzar este objetivo dependen de varios factores, entre ellos el número total de resultados, temas específicos de seguridad, asesoramiento de riesgos de la aplicación, etc. Además de decidir si un resultado representa un problema de seguridad válido, el proceso de selección también implica la modificación de atributos de resultados (gravedad, tipo, clasificación) cuando proceda.

La estrategia de selección es importante para garantizar que se consiguen los objetivos en el orden y el periodo de tiempo que desee. La mejor forma de realizar la selección es de forma iterativa, evaluando un subconjunto de resultados y determinando la disposición de cada subconjunto en cada iteración. Existen varios enfoques para decidir cómo definir las iteraciones de la selección. Uno de ellos consiste en crear subconjuntos de resultados de alto riesgo en función de la gravedad general. Podría empezar solucionando los resultados que potencialmente presentan un mayor riesgo y luego aquellos que presentan un riesgo menor probable. Otro enfoque consiste en definir subconjuntos en función de la seguridad, como por ejemplo Inyección de SQL o Validación necesaria.

Generalmente, un analista de seguridad o un auditor de IT realiza la selección. El analista o auditor puede enviar los resultados que requieren cambios en el código a un sistema de seguimiento de defectos y luego a los desarrolladores para su remediación. En otros casos, los desarrolladores pueden seleccionar y resolver problemas.

Durante la fase de selección, puede:

- Revisar los resultados con tipos de vulnerabilidad especialmente interesantes
- Ver las API de una determinada categoría
- Comparar resultados en distintos asesoramientos
- Filtrar o excluir resultados específicos
- Cambiar el tipo de gravedad o de vulnerabilidad de un resultado
- Ascender resultados de cobertura de escaneo y sospechosos a definitivos
- Anotar resultados
- Enviar defectos a sistemas de rastreo de defectos o enviar los resultados a otros por correo electrónico.

AppScan Source proporciona todas las herramientas necesarias para analizar los resultados utilizando diferentes estrategias de selección. El filtrado ofrece un método para ver únicamente los resultados que se deben procesar dentro de una determinada iteración de selección. Si la estrategia iterativa se realiza por gravedad y clasificación, puede filtrar los resultados desde la vista Matriz de vulnerabilidad. Si la estrategia iterativa se realiza por tipo de vulnerabilidad, puede filtrar los

resultados desde la vista Resumen de asesoramiento. AppScan Source for Analysis también proporciona un editor de filtros que da soporte a los enfoques iterativos complejos.

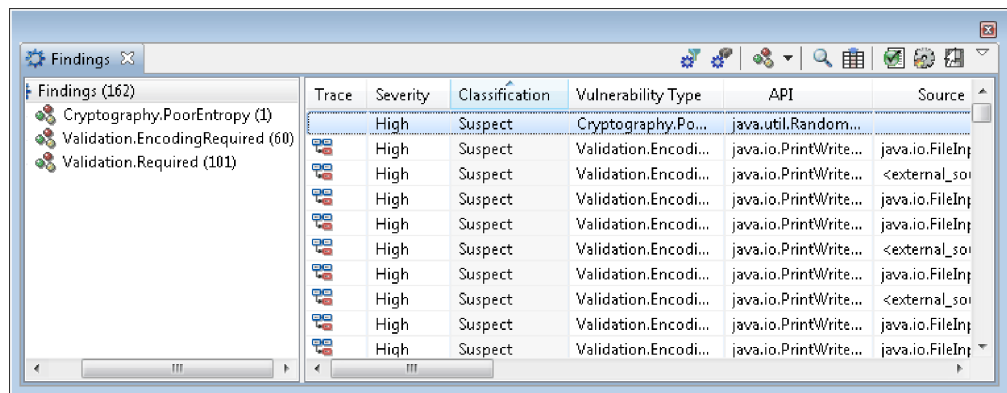
Una vez seleccionado el enfoque de selección, AppScan Source for Analysis da soporte a la disposición de los resultados.

- Ecluir resultados individuales o colecciones de resultados
- Modificar los detalles del resultado (tipo, gravedad, clasificación)
- Crear paquetes (un mecanismo de agrupación para resultados)
- Comparar asesoramientos con la vista Diferencia entre asesoramientos

## Visualización de resultados

La vista Resultados, o cualquier vista con resultados, muestra un árbol de resultados (una agrupación jerárquica de criterios de asesoramiento) y una tabla de resultados para cada escaneo. El elemento que se haya seleccionado en el árbol de resultados determina los resultados que aparecen en la tabla.

Si selecciona la raíz del árbol se muestran todos los resultados en la tabla y si selecciona un tipo de agrupación se muestran solo estos tipos de resultados.



| Trace | Severity | Classification | Vulnerability Type   | API                   | Source             |
|-------|----------|----------------|----------------------|-----------------------|--------------------|
|       | High     | Suspect        | Cryptography.Po...   | java.util.Random...   |                    |
|       | High     | Suspect        | Validation.Encodi... | java.io.PrintWrite... | java.io.FileInp... |
|       | High     | Suspect        | Validation.Encodi... | java.io.PrintWrite... | <external_soi...   |
|       | High     | Suspect        | Validation.Encodi... | java.io.PrintWrite... | java.io.FileInp... |
|       | High     | Suspect        | Validation.Encodi... | java.io.PrintWrite... | <external_soi...   |
|       | High     | Suspect        | Validation.Encodi... | java.io.PrintWrite... | java.io.FileInp... |
|       | High     | Suspect        | Validation.Encodi... | java.io.PrintWrite... | <external_soi...   |
|       | High     | Suspect        | Validation.Encodi... | java.io.PrintWrite... | java.io.FileInp... |
|       | High     | Suspect        | Validation.Encodi... | java.io.PrintWrite... | java.io.FileInp... |

AppScan Source for Analysis muestra los resultados por distintas agrupaciones, que incluyen:

- **Tipo de vulnerabilidad**
- **Clasificación**
- **Archivo**
- **Fuente**
- **Receptor**
- **API**
- **Paquetes**
- **CWE**
- **Tabla**

**Nota:** La clasificación y la gravedad se clasifican en orden descendente de forma predeterminada. Las demás columnas se clasifican en orden ascendente.

Estas columnas aparecen en una tabla de resultados.

Tabla 11. Tabla Resultados

| Cabecera de columna    | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rastreo                | Un icono en esta columna indica que existe un rastreo para salidas perdidas o conocidas.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Gravedad               | <ul style="list-style-type: none"> <li>• <b>Alta</b> : Supone un riesgo para la confidencialidad, integridad o disponibilidad de los datos o la integridad o disponibilidad de los recursos de proceso. A las condiciones de gravedad alta debe dárseles prioridad para su remediación inmediata.</li> <li>• <b>Media</b> : Supone un riesgo para la seguridad de los datos o la integridad de los recursos, pero la condición es menos susceptible de ser atacada. Las condiciones de seguridad media deben revisarse y resolverse cuando sea posible.</li> <li>• <b>Baja</b> : Supone un riesgo mínimo para la seguridad de los datos o la integridad de los recursos.</li> <li>• <b>Información</b> : El resultado, en sí mismo, no es susceptible de ser comprometido. Sino que describe las tecnologías, las características de la arquitectura o los mecanismos de seguridad utilizados en el código.</li> </ul> |
| Clasificación          | <p>Tipo de resultado: resultado de seguridad <b>Definitivo</b> o <b>Sospechoso</b> o resultado de <b>Cobertura de escaneo</b>.</p> <p><b>Nota:</b> En algunos casos, se puede utilizar una clasificación de <b>Ninguno</b> para denotar una clasificación que no corresponde a un resultado de seguridad ni a un resultado de cobertura de escaneo.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Tipo de vulnerabilidad | Categoría de vulnerabilidad, como por ejemplo <code>Validation.Required</code> o <code>Injection.SQL</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| API                    | La llamada vulnerable, mostrando la API y los argumentos que se le pasan.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Fuente                 | Un origen es una entrada para el programa, como un archivo, una solicitud de servlet, una entrada de consola o un socket. En la mayoría de los orígenes de entrada, los datos devueltos son ilimitados en términos de contenido y longitud. Cuando se deselectiona una entrada, se considera que está corrupta.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Receptor               | Una salida puede tener cualquier formato externo en el que puedan escribirse datos. Como ejemplo de salida cabe citar las bases de datos, los archivos, la salida de la consola y los sockets. Escribir datos en una salida sin verificarla puede ser indicio de una grave vulnerabilidad de seguridad.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

Tabla 11. Tabla Resultados (continuación)

| Cabecera de columna | Descripción                                                                                                                                                                                                                      |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Directorio          | Vía de acceso completa de los archivos escaneados.                                                                                                                                                                               |
| Archivo             | Nombre del archivo de código donde se presenta el resultado de cobertura de escaneo o el resultado de seguridad. Las vías de acceso de archivos en los resultados son relativas al directorio de trabajo del proyecto escaneado. |
| Método de llamada   | La función (o método) desde la que se realiza la llamada vulnerable.                                                                                                                                                             |
| Línea               | Número de línea en el archivo de código que contiene la API vulnerable.                                                                                                                                                          |
| Paquetes            | Paquete que contiene este resultado.                                                                                                                                                                                             |
| CWE                 | ID y tema del diccionario desarrollado por la comunidad que recoge las debilidades comunes del software (temas de CWE (Common Weakness Enumeration)).                                                                            |

**Nota:** Si selecciona un resultado para el que AppScan Source no puede ubicar el origen, se le preguntará con un recuadro de diálogo si desea ser advertido cuándo no es posible ubicar los archivos de origen. Si selecciona **Sí**, será advertido cada vez que se seleccione un resultado para el que no es posible ubicar los archivos de origen. Si selecciona **No**, no se le indicará. Este valor persiste mientras el asesoramiento actual permanezca abierto. El valor se restablece cada vez que se abre el asesoramiento o si sale de AppScan Source.

## El proceso de selección de AppScan Source

El proceso de selección incluye la manipulación de resultados mediante paquetes, filtros y exclusiones y la comparación de los resultados del asesoramiento.

### Filtros

Un *filtro* es un conjunto de reglas que define resultados con ciertos rasgos. Un filtro le permite presentar una vista dinámica de estos resultados y le permite seleccionar resultados similares.

Los filtros pueden ser *compartidos* o *locales*:

- Los filtros compartidos residen en el servidor de AppScan. Cualquiera que esté conectado a dicho servidor puede utilizar el filtro.
- Los filtros locales residen en el sistema local.

### Paquetes

Un *paquete* es una colección con nombre de resultados individuales que se almacena con una aplicación. Un paquete se crea simplemente seleccionando los resultados y añadiéndolos a un paquete nuevo o existente.

La agrupación de resultados similares en paquetes permite a los analistas de seguridad segmentar y seleccionar problemas del código fuente. Puede enviar paquetes a un sistema de seguimiento de defectos o puede enviar por correo

electrónico los resultados a los desarrolladores para que los revisen como parte del proceso de selección y análisis.

## Exclusiones

Una *exclusión* omite resultados de escaneos. AppScan Source tiene un **Paquete excluido** incorporado, el cual contiene los resultados que ha excluido (por ejemplo, debido a que no requieren resolución).

**Nota:** Los resultados excluidos de los resultados de asesoramiento no contribuyen al cálculo de las métricas de una aplicación o de un proyecto.

## Resultados modificados

Un resultado *modificado* es un resultado con un tipo de vulnerabilidad, una gravedad o una clasificación alterados. Si añade notas a un resultado, también se considera que el resultado se ha modificado.

## Comparación de asesoramientos

En AppScan Source for Analysis, los asesoramientos se comparan utilizando la acción **Diferencia entre asesoramientos**. Cuando se comparan dos asesoramientos, las diferencias entre ambos se visualizan en la vista Diferencia entre asesoramientos (que parece una combinación de la vista Mis asesoramientos y la vista Resultados).

**Nota:** Cuando se comparan los asesoramientos, se omiten los filtros y paquetes.

---

## Selección de ejemplo

En este ejemplo se describe un flujo de trabajo de selección de AppScan Source utilizado por un analista de seguridad. El flujo de trabajo de selección puede variar en función de los requisitos de la empresa.

Mr. Jones, el analista de seguridad de la empresa, desea realizar una selección de los resultados de su escaneo. Desea agrupar y establecer prioridades entre los resultados similares y luego enviarlos al desarrollador adecuado para su resolución.

En primer lugar, Mr. Jones escanea el código fuente de su aplicación y, a continuación, abre el asesoramiento en la perspectiva Selección. El escaneo genera unos 2.000 resultados, todos los cuales puede revisar en la vista Resultados. Sin embargo, Mr. Jones desea obtener en primer lugar una visión general de los resultados y abre la vista Matriz de vulnerabilidad que muestra el desglose por gravedad y tipo de resultado (seguridad o cobertura de escaneo). Los resultados de cobertura de escaneo y los resultados de seguridad sospechosos requieren más investigación para determinar el riesgo.

En la Matriz de vulnerabilidad, Mr. Jones detecta ocho resultados de seguridad definitivos de gravedad alta. Pulsa el cuadro de la matriz que indica ocho resultados definitivos, creando de forma automática un filtro y haciendo que la vista Resultados se renueve para visualizar únicamente estos ocho problemas críticos. Mr. Jones decide tratar estos problemas como errores. Selecciona los ocho y los envía a su sistema de seguimiento de defectos. Luego restablece este filtro desde la Matriz de vulnerabilidad.

A continuación, Mr. Jones se centra en la vista Resumen de asesoramiento. Observa que los 2.000 resultados constan de más de media docena de tipos de vulnerabilidad. Decide concentrarse en los problemas de validación y crea otro filtro desde la vista Resumen de asesoramiento. Pulsa `Validation.EncodingRequired` y `Validation.Required` en el gráfico y reduce el número de resultados de la vista Resultados a unos 500 resultados.

Quinientos resultados siguen resultando difíciles de seleccionar. Mr. Jones decide filtrar más los resultados. En la vista Editor de filtros, aumenta el filtro creado desde el Resumen de asesoramiento con el requisito de gravedad alta. Ahora la tabla de resultados muestra 150 entradas.

Cuando clasifica por nombre de archivo, observa que algunos de los resultados están en código procedente de una biblioteca de otro proveedor. Mr. Jones sabe que el uso de esta biblioteca es un hecho aislado y que no tiene intención de solucionar sus problemas de seguridad. Excluye estos resultados, lo que hace que la vista Resultados y las métricas se actualicen inmediatamente. Futuros escaneos detectarán estos resultados, pero están segregados y no contribuirán a las métricas.

Mr. Jones observa que hay varios resultados de seguridad sospechosos de gravedad alta del tipo `Validation.Required`. Sabe que los datos se están consumiendo sin validación. Decide ascender estos resultados de sospechosos a definitivos. Mientras realiza esta modificación, decide añadir notas para explicar los cambios, y luego se envía por correo electrónico estos resultados a sí mismo como recordatorio para dar prioridad a su solución o revisarlos en la vista Resultados modificados.

A continuación, Mr. Jones vuelve a clasificar por nombre de archivo y se da cuenta de que algunos de los resultados están en el servidor de fondo y otros están en la interfaz de usuario. Selecciona todos los resultados de fondo y crea un nuevo paquete, llamado Backend Server - Validation Required. Selecciona el resto de los resultados y los coloca en un paquete llamado UI - Validation Required. La selección continúa, centrándose en los tipos `Validation.EncodingRequired` con gravedad alta.

Al final del día, Mr. Jones ha creado una docena de paquetes. Durante el día, utiliza el gráfico, filtros y la matriz de vulnerabilidad para reducir los resultados a un número que pueda gestionar simultáneamente en una vista. A veces coloca estos resultados individuales en paquetes. Otras veces excluye los resultados que no son importantes. En otras ocasiones, crea nuevos paquetes para resultados específicos; a veces añade resultados a un paquete existente.

Ahora Mr. Jones revisa la docena de paquetes. Determina que debe enviar los paquetes Backend Server - Validation Required y UI - Validation Required a su sistema de seguimiento de defectos para notificar a los desarrolladores estas áreas que le preocupan.

Mr. Jones va a la vista Paquetes y abre el paquete Backend Server - Validation Required. Se abre una nueva vista llamada **Backend Server - Validation Required** con una lista de los resultados que ha colocado en el paquete. Luego envía este paquete a un sistema de seguimiento de defectos. Luego, por la noche, cuando el desarrollador inicia una sesión en Rational ClearQuest y ve los errores que se le han asignado, puede abrir el resultado en AppScan Source for Development.

Mr. Jones revisa los otros paquetes. Envía algunos al sistema de seguimiento de defectos y envía otros por correo electrónico a sus compañeros. Sin embargo,

algunos paquetes contienen resultados que, tras otra revisión, no considera tan importantes. Mueve estos resultados menos importantes a dos paquetes, By Design e Irrelevant. Mr. Jones ha determinado que estos resultados son aceptables y no tiene intención de modificar el código. Además de los resultados By Design e Irrelevant, Mr. Jones se da cuenta de que los resultados Cryptography.PoorEntropy tampoco le importan mucho. Sabe que la entropía puede ser pobre para estas llamadas de criptografía y, aunque un sistema rápido podría adivinar la clave en menos de una semana, esto no es importante para una aplicación en la que los datos dejan de resultar útiles unas horas después de su cifrado. Mr. Jones también desea eliminar estos resultados.

Añade los paquetes By Design e Irrelevant a la lista de **Paquetes excluidos** en la vista Propiedades. También abre el Editor de filtros y crea otro filtro con el tipo de vulnerabilidad, Cryptography.PoorEntropy, guarda el filtro denominado Crypto, y establece el comportamiento del filtro Crypto en **Invertido** (en el recuadro de diálogo Seleccionar filtro, elige **Invertir filtro**). Luego inicia un escaneo y se va a su casa. Las métricas no reflejan estas exclusiones hasta después del siguiente escaneo.

---

## Selección con filtros

AppScan Source for Analysis notifica todas las vulnerabilidades de seguridad potenciales y puede generar varios miles de resultados para un código base mediano o grande. Cuando realice un escaneo, es posible que encuentre que la lista de resultados contiene elementos que no le interesan. Para eliminar ciertos resultados de la vista Resultados, puede elegir un filtro predefinido o puede crear su propio *filtro*. Un filtro especifica los criterios que determinan qué resultados se deben eliminar de la vista.

- “Visión general del filtro ”
- “Reglas de filtro” en la página 152
- “Ejemplos de filtro” en la página 154

### Visión general del filtro

Los filtros eliminan o restringen elementos que cumplen los criterios determinados por las reglas de filtro y ayudan a gestionar resultados de escaneo durante la selección o el informe. Un filtro ayuda a guiar el flujo de trabajo y a centrar el análisis de seguridad en las áreas más críticas de un subconjunto de resultados. Por ejemplo, durante el examen del código, un analista puede crear un filtro que evite ver los resultados de gravedad baja. Como alternativa, es posible que el analista prefiera excluir las vulnerabilidades de los archivos include de la biblioteca del sistema. Un filtro puede eliminar estos elementos de la vista, y puede excluir archivos individuales o los archivos que ya se han investigado con anterioridad.

Los filtros se pueden aplicar antes o después del escaneo:

- Para aplicar filtros antes del escaneo, establezca filtros globales en propiedades de aplicaciones o de proyectos. O bien, escanee con una configuración de escaneo que incluya filtros. Al aplicar filtros antes del escaneo, no podrá mostrar resultados no filtrados ni eliminar el filtro sin escanear de nuevo.
- Varias vistas (en concreto, la vista Editor de filtros) le permite aplicar filtros tras escanear. Cuando se utilicen estas vistas para el filtrado, todos los elementos filtrados permanecerán en los resultados de escaneo, pero sólo aparecerán en la vista Resultados si se selecciona el conmutador **Mostrar resultados filtrados** (icono  ).

AppScan Source incluye varios filtros predefinidos que se pueden seleccionar para filtrar resultados de escaneo.

Cuando tenga un filtro, puede definir una propiedad que convierta el filtro en una *exclusión*. Una exclusión afecta a los escaneos y elimina todos los resultados que coinciden con el filtro o, alternativamente, todos los resultados que no coincidan con el filtro.

## Reglas de filtro

Cada filtro consta de reglas que definen qué resultados hay que restringir (inclusión) o eliminar (excluir) de los resultados de la tabla de resultados (para reglas de rastreo, puede restringir o eliminar en base a las propiedades de rastreo).

- Una regla de **Restringido para** (regla incluyente) excluye los resultados que no tienen los criterios especificados y elimina dichos resultados de los resultados visibles de la tabla de resultados.
- Una regla de **eliminación** (regla excluyente) elimina los resultados que contienen criterios de los resultados del escaneo. Una regla de eliminación excluye los resultados que tienen los criterios especificados y elimina dichos resultados de los resultados visibles.

Una regla de filtro puede incluir estas características:

- **Gravedad:** identifica el impacto o riesgo potencial de los valores individuales. Las reglas de gravedad son únicamente de restricción.
  - **Alta** : Supone un riesgo para la confidencialidad, integridad o disponibilidad de los datos o la integridad o disponibilidad de los recursos de proceso. A las condiciones de gravedad alta debe dárseles prioridad para su remediación inmediata.
  - **Media** : Supone un riesgo para la seguridad de los datos o la integridad de los recursos, pero la condición es menos susceptible de ser atacada. Las condiciones de seguridad media deben revisarse y resolverse cuando sea posible.
  - **Baja** : Supone un riesgo mínimo para la seguridad de los datos o la integridad de los recursos.
  - **Información** : El resultado, en sí mismo, no es susceptible de ser comprometido. Sino que describe las tecnologías, las características de la arquitectura o los mecanismos de seguridad utilizados en el código.
- **Clasificación:** filtra los resultados en base a las clasificaciones descritas en este tema. Las reglas de clasificación son únicamente de restricción.
- **Tipo de vulnerabilidad:** filtrar por una determinada categoría de vulnerabilidad, como por ejemplo BufferOverflow. Cuando añade un tipo de vulnerabilidad, puede seleccionar entre todos los tipos de vulnerabilidad posibles o puede elegir solo entre los tipos que se ha encontrado en el asesoramiento actual. Para elegir entre los tipos de vulnerabilidad que se han encontrado en el asesoramiento actual, seleccione **Mostrar solo los valores de asesoramientos abiertos** en el cuadro de diálogo Seleccionar valores.

Seleccionar entre todos los tipos de vulnerabilidad posibles es útil cuando se crea un filtro para futuros escaneos. Para mostrar todos los tipos de vulnerabilidad, deselectione **Mostrar solo los valores de asesoramientos abiertos** (si no hay asesoramientos abiertos, todos los tipos de vulnerabilidad se muestran de forma predeterminada y el recuadro de selección **Mostrar solo los valores de asesoramientos abiertos** no está disponible).

- **API:** filtrar todas las vulnerabilidades de una determinada API.



- **Archivo:** filtrar todas las vulnerabilidades de un determinado archivo.
- **Directorio:** filtrar todas las vulnerabilidades de un determinado directorio.
- **Proyecto:** filtrar todas las vulnerabilidades de un determinado directorio.
- **Rastreo:** le permite filtrar los resultados en función de propiedades de rastreo (consulte “Entradas y salidas” en la página 193 para obtener más información sobre las propiedades de rastreo). Los filtros pueden incluir reglas de rastreo que restrinjan o eliminen en función de las propiedades de rastreo. Cuando pulsa **Añadir** en alguna de estas secciones (restringir o eliminar), se abre el recuadro de diálogo Entrada de regla de rastreo. Aquí puede especificar:

- **Origen:** en el campo **Expresión regular de API** de la sección Origen, especifique el origen de rastreo o una expresión regular que cubra varios orígenes (la entrada predeterminada es `.*`, la expresión regular o carácter comodín que devolverá todo). Si utiliza una expresión regular, seleccione el tipo en el menú del campo **Tipo de expresión regular** (el tipo de expresión regular predeterminado es PERL). Si no utiliza una expresión regular, seleccione **Coincidencia exacta** en el menú del campo **Tipo de expresión regular**.

Si la entrada **Expresión regular de API** es una expresión válida, aparece un icono con una marca de selección verde junto al campo. Si la entrada no es una expresión válida, aparece un icono con una X roja junto al campo y el botón **Aceptar** del cuadro de diálogo aparece inhabilitado. Si mueve el cursor sobre cualquiera de los iconos verá más información sobre los resultados de la validación. Si ha realizado seleccionado una entrada que no es una expresión válida pero desea continuar utilizándola, marque el cuadro de selección **Ignorar los errores de validación anteriores** que hay en la parte inferior del cuadro de diálogo. Esto habilitará el botón **Aceptar** del cuadro de selección (siempre y cuando la expresión no esté vacía) y el icono que hay junto a la expresión no válida se convertirá en una marca de comprobación verde con el texto flotante **Validación inhabilitada**.

También puede refinar el filtro utilizando el botón **Añadir una propiedad VMAT** en la sección Propiedades de origen (más adelante encontrará información adicional sobre las propiedades VMAT), sin embargo al utilizar esta característica para limitar por vulnerabilidad no tendrá el efecto deseado puesto que el tipo de vulnerabilidad viene determinado por el receptor ("sink") y no por el origen.

- **Receptor:** en la sección Receptor, puede añadir receptores como filtros del mismo modo en que se especifican orígenes.

Es posible refinar el filtrado limitándolo a tipos de vulnerabilidad específicos (para limitar el efecto de la entrada de la regla de rastreo especifique a tan sólo tipos de vulnerabilidad, mecanismos o tecnologías). Para ello, pulse **Añadir una propiedad VMAT** en la sección Propiedades de receptor ("Sink") y seleccione la propiedad en el recuadro de diálogo Elegir propiedades. La lista de propiedades se puede filtrar utilizando el campo **Filtro**.

VMAT es una categorización de los cuatro principales tipos de propiedades que AppScan Source aplica a las interfaces de programación de aplicaciones (API). Las categorías de propiedades de VMAT incluyen:

- **Vulnerabilidad:** el tipo de vector de aprovechamiento o ataque que da lugar a una violación de seguridad
- **Mecanismo:** el control de seguridad utilizado para evitar una vulnerabilidad
- **Atributo:** estas propiedades no están disponibles actualmente en el cuadro de diálogo Elegir propiedades

- **Tecnología:** la descripción general del tipo de funcionalidad que proporciona una API

**Ejemplo de filtro:** Para filtrar por todas las inyecciones de SQL y XSS provenientes desde HTTP (el origen de riesgo más elevado), cree una regla de rastreo **Restringir a** que contenga el filtro `Technology.Communications.HTTP` en la sección Propiedades de origen y las reglas `Vulnerability.Injection.SQL` y `Vulnerability.CrossSiteScripting` en la sección Propiedades de receptor.

- **Llamadas necesarias:** en la sección Llamadas necesarias, añada llamadas de API específicas que deben estar en la vía de acceso entre el origen y el receptor. Las llamadas necesarias limitan los resultados a aquellos que tienen rastreos que pasan a través de las llamadas necesarias especificadas. Cuando pulsa **Añadir una llamada intermedia**, se abre el cuadro de diálogo Configurar API. En este cuadro de diálogo, especifique la llamada del mismo modo en que se especifican orígenes y receptores.
- **Llamadas prohibidas:** en la sección Llamadas prohibidas, añada llamadas de API específicas que no deben estar en la vía de acceso entre el origen y el receptor. Las llamadas prohibidas limitan los resultados a aquellos que tienen rastreos que no pasan a través de las llamadas prohibidas especificadas. Las llamadas prohibidas se añaden del mismo modo que las llamadas necesarias.

#### Consejo:

- Al filtrar por **Tipo de vulnerabilidad, API, Archivo, Directorio, o Proyecto**, la lista que se muestra en el cuadro de diálogo Seleccionar valores puede filtrarse si se escribe un patrón en el campo de filtro en la parte superior del recuadro de diálogo.
- En cualquier tabla de resultados, busque las columnas **Origen y Receptor** para ver los orígenes y receptores que desea filtrar.
- Para obtener una idea de las propiedades de origen, receptor y llamada que desea filtrar, observe la columna **Tipo de vulnerabilidad** de cualquier tabla de resultados.
- Para ver las llamadas que quizás desee filtrar, observe las entradas de la columna **API** de cualquier tabla de resultados.

## Ejemplos de filtro

Tabla 12. Ejemplos de filtro

| Comportamiento del filtro en una tabla de resultados                                           | Valores de filtro en la vista Editor de filtros                                                                                                                                                                                                                                                           |
|------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| La tabla de resultados incluye únicamente resultados de seguridad sospechoso de gravedad alta. | <ul style="list-style-type: none"> <li>• En la sección Gravedad, marque el cuadro de selección <b>Alto</b> y desmarque los demás cuadros de selección.</li> <li>• En la sección Clasificación, marque el recuadro de selección <b>Sospechoso</b> y desmarque los demás recuadros de selección.</li> </ul> |

Tabla 12. Ejemplos de filtro (continuación)

| Comportamiento del filtro en una tabla de resultados                                                                                               | Valores de filtro en la vista Editor de filtros                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>La tabla de resultados incluye todos los resultados de un proyecto llamado ProjectA, con la excepción de las vulnerabilidades de tipo info.</p> | <ul style="list-style-type: none"> <li>• En la sección Tipo de vulnerabilidad, seleccione el botón de selección <b>Eliminar</b> y pulse <b>Añadir</b>. En el cuadro de diálogo Seleccionar valores, seleccione <b>Vulnerability.Info</b>.</li> <li>• En la sección Proyecto, seleccione el botón de selección <b>Restringido para</b> y pulse <b>Añadir</b>. En el cuadro de diálogo Seleccionar valores, seleccione ProjectA.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                               |
| <p>Solo se muestran los resultados con un rastreo.</p>                                                                                             | <p>En la sección Rastreo, pulse <b>Añadir</b> en la sección de <b>Restringido para</b>. Acepte las entradas predeterminadas del cuadro de diálogo Entrada de regla de rastreo y pulse <b>Aceptar</b>. Los valores predeterminados del cuadro de diálogo son:</p> <ul style="list-style-type: none"> <li>• El campo <b>Expresión regular de API</b> del origen es <b>.*</b> y el tipo de expresión regular es <b>PERL</b>. Esto indica a AppScan Source que debe filtrar los resultados con un origen (utilizando la sintaxis de expresión regular de Perl).</li> <li>• El campo <b>Expresión regular de API</b> del receptor es <b>.*</b> y el tipo de expresión regular es <b>PERL</b>. Esto indica a AppScan Source que debe filtrar los resultados con un receptor (utilizando la sintaxis de expresión regular de Perl).</li> </ul> |

Tabla 12. Ejemplos de filtro (continuación)

| Comportamiento del filtro en una tabla de resultados                                                                                                                              | Valores de filtro en la vista Editor de filtros                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| La tabla de resultados muestra orígenes relacionados con HTTP con receptores relacionados con Inyección de SQL que no pasan a través de <code>java.lang.Integer.parseInt</code> . | <p>En la sección Rastreo, pulse <b>Añadir</b> en la sección de <b>Restringido para</b>. En el cuadro de diálogo Entrada de regla de rastreo, siga estos pasos:</p> <ul style="list-style-type: none"> <li>• En la sección Origen, pulse <b>Añadir una propiedad VMAT</b>. En el cuadro de diálogo Elegir propiedades, seleccione <code>Technology.Communications.HTTP</code>. Pulse <b>Aceptar</b> para añadir la propiedad VMAT y vuelva al cuadro de diálogo Entrada de regla de rastreo.</li> <li>• En la sección Receptor, pulse <b>Añadir una propiedad VMAT</b>. En el cuadro de diálogo Elegir propiedades, seleccione <code>Vulnerability.Injection.SQL</code>. Pulse <b>Aceptar</b> para añadir la propiedad VMAT y vuelva al cuadro de diálogo Entrada de regla de rastreo.</li> <li>• En la sección Llamadas prohibidas, pulse <b>Añadir una llamada intermedia</b>. En el cuadro de diálogo Configurar API, especifique <code>java.lang.Integer.parseInt.*</code> en el campo <b>Expresión regular de API</b>. Pulse <b>Aceptar</b> para añadir la llamada intermedia y vuelva al cuadro de diálogo Entrada de regla de rastreo y pulse <b>Aceptar</b> para añadir la entrada de regla de rastreo.</li> </ul> |

## Utilización de filtros predefinidos de AppScan Source

AppScan Source incluye un conjunto de filtros predefinidos que se pueden seleccionar para filtrar resultados de escaneo. En este tema de ayuda se describen estos filtros.

**Nota:** En AppScan Source Versión 8.8, se mejoraron los filtros predefinidos para proporcionar mejores resultados de escaneo. Si necesita continuar utilizando los filtros predefinidos de versiones anteriores de AppScan Source (los filtros archivados se encuentran listados en “Filtros predefinidos de AppScan Source (Versión 8.7.x y anteriores)” en la página 159), siga las instrucciones en “Restauración de filtros predefinidos archivados” en la página 161.

**Nota:** En AppScan Source for Development (plugin de Visual Studio), esta vista forma parte de la ventana Editar filtros.

- “! - Los pocos vitales de AppScan” en la página 157
- “! - Orígenes de riesgo alto” en la página 157
- “! - Tipos importantes” en la página 157
- “Vulnerabilidades CWE SANS Top 25 2010” en la página 158
- “Comunicaciones externas” en la página 158
- “Informativos y gravedad baja” en la página 158
- “Ruido - Calidad” en la página 158

- “Vulnerabilidades OWASP Mobile Top 10” en la página 158
- “Vulnerabilidades OWASP Top 10 2010” en la página 158
- “Vulnerabilidades OWASP Top 10 2013” en la página 159
- “Vulnerabilidades PCI Data Security Standard” en la página 159
- “Vulnerabilidades EncodingRequired para orígenes HTTP” en la página 159
- “Vulnerabilidades de validación requerida para receptores (sink) C/C++” en la página 159
- “Orígenes de confianza” en la página 159
- “Vulnerabilidades sin rastreo” en la página 159

## ! - Los pocos vitales de AppScan

Este filtro compara resultados procedentes de algunas de las categorías de vulnerabilidad más peligrosas. Los resultados se limitan a las vulnerabilidades de gravedad media y alta. Los resultados con orígenes específicos se eliminan de los resultados. Las categorías de vulnerabilidad específicas que se incluyen en este filtro son:

```
Vulnerability.CrossSiteScripting
Vulnerability.CrossSiteScripting.Reflected
Vulnerability.CrossSiteScripting.Stored
Vulnerability.Injection.OS
Vulnerability.Injection.LDAP
Vulnerability.Injection.SQL
Vulnerability.Injection.Mail
```

## ! - Orígenes de riesgo alto

Este filtro limita los resultados a orígenes y tipos de vulnerabilidad con una de estas propiedades:

```
Technology.Communications.HTTP
Technology.Communications.IP
Technology.Communications.RCP
Technology.Communications.TCP
Technology.Communications.UDP
Technology.Communications.WebService
```

## ! - Tipos importantes

Este filtro contiene resultados de una amplia gama de categorías de vulnerabilidad importantes. Los resultados están restringidos a las gravedades media y alta con clasificaciones de Sospechoso o Definitivo. Las categorías específicas que se incluyen en este filtro son:

```
Vulnerability.AppDOS
Vulnerability.Authentication.Credentials.Unprotected
Vulnerability.BufferOverflow
Vulnerability.BufferOverflow.FormatString
Vulnerability.BufferOverflow.ArrayIndexOutOfBounds
Vulnerability.BufferOverflow.BufferSizeOutOfBounds
Vulnerability.BufferOverflow.IntegerOverflow
Vulnerability.BufferOverflow.Internal
Vulnerability.CrossSiteRequestForgery
Vulnerability.CrossSiteScripting
Vulnerability.CrossSiteScripting.Reflected
Vulnerability.CrossSiteScripting.Stored
Vulnerability.FileUpload
Vulnerability.Injection
Vulnerability.Injection.LDAP
Vulnerability.Injection.OS
```

Vulnerability.Injection.SQL  
Vulnerability.Injection.XML  
Vulnerability.Injection.XPath  
Vulnerability.Malicious.EasterEgg  
Vulnerability.Malicious.Trigger  
Vulnerability.Malicious.Trojan  
Vulnerability.PathTraversal  
Vulnerability.Validation.EncodingRequired  
Vulnerability.Validation.EncodingRequired.Struts

## **Vulnerabilidades CWE SANS Top 25 2010**

Este filtro se centra en los tipos de vulnerabilidad relacionados con los *CWE/SANS TOP 25 Most Dangerous Software Errors* para 2010.

Para obtener más información sobre los *25 errores de software más peligrosos de CWE/SANS 2011*, consulte <http://cwe.mitre.org/top25/>.

## **Comunicaciones externas**

Este filtro compara los resultados que se originan fuera de la aplicación y en una red. Este filtro compara resultados que se originan en cualquier origen de tipo *Technology.Communications*.

## **Informativos y gravedad baja**

Este filtro contiene los resultados con gravedad baja e informativa. Están incluidas todas las clasificaciones (Definitivos, Sospechosos y Cobertura de escaneo).

## **Ruido - Calidad**

Este filtro hace que los resultados sólo incluyan tipos de vulnerabilidades relacionados con prácticas de codificación de calidad.

## **Vulnerabilidades OWASP Mobile Top 10**

Este filtro se centra en los tipos de vulnerabilidad relacionados con la lista Open Web Application Security Project (OWASP) Mobile Top 10 Release Candidate v1.0.

Para obtener más información acerca de OWASP, consulte [https://www.owasp.org/index.php/Main\\_Page](https://www.owasp.org/index.php/Main_Page). Los enlaces a varios documentos OWASP y de riesgos de seguridad están disponibles en [https://www.owasp.org/index.php/Category:OWASP\\_Top\\_Ten\\_Project](https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project).

## **Vulnerabilidades OWASP Top 10 2010**

Este filtro se centra en los tipos de vulnerabilidad relacionados con la lista Open Web Application Security Project (OWASP) Top 10 2010.

Para obtener más información acerca de OWASP, consulte [https://www.owasp.org/index.php/Main\\_Page](https://www.owasp.org/index.php/Main_Page). Los enlaces a varios documentos OWASP y de riesgos de seguridad están disponibles en [https://www.owasp.org/index.php/Category:OWASP\\_Top\\_Ten\\_Project](https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project).

## **Vulnerabilidades OWASP Top 10 2013**

Este filtro se centra en los tipos de vulnerabilidad relacionados con la lista Open Web Application Security Project (OWASP) Top 10 2013.

Para obtener más información acerca de OWASP, consulte [https://www.owasp.org/index.php/Main\\_Page](https://www.owasp.org/index.php/Main_Page). Los enlaces a varios documentos OWASP y de riesgos de seguridad están disponibles en [https://www.owasp.org/index.php/Category:OWASP\\_Top\\_Ten\\_Project](https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project).

## **Vulnerabilidades PCI Data Security Standard**

Este filtro se centra en los tipos de vulnerabilidad relacionados con el estándar Payment Card Industry Data Security Standard (PCI DSS) Versión 3.2.

Consulte el apartado [https://www.pcisecuritystandards.org/security\\_standards/index.php](https://www.pcisecuritystandards.org/security_standards/index.php) para obtener más información.

## **Resultados de cobertura de escaneo**

Este filtro hace que los resultados sólo incluyan Resultados de cobertura de escaneo (consulte “Clasificaciones” en la página 21 para obtener más información).

## **Vulnerabilidades EncodingRequired para orígenes HTTP**

Este filtro se centra en los resultados de las categorías de vulnerabilidad de Validation.EncodingRequired y Validation.EncodingRequired.Struts. Se incluyen únicamente los resultados originados de un origen Technology.Communications.HTTP. Los resultados están limitados a las gravedades media y alta con clasificaciones de Sospechoso o Definitivo.

## **Vulnerabilidades de validación requerida para receptores (sink) C/C++**

Este filtro se centra en vulnerabilidades Validation.Required para un conjunto conocido de receptores (sink) de C y C++. Los resultados están limitados a las gravedades media y alta con clasificaciones de Sospechoso o Definitivo.

## **Orígenes de confianza**

En este filtro se presupone que los datos que provienen de determinados orígenes como, por ejemplo, objetos de sesión o atributos de solicitud, son seguros.

## **Vulnerabilidades sin rastreo**

Este filtro lista vulnerabilidades que no contienen rastreos.

## **Filtros predefinidos de AppScan Source (Versión 8.7.x y anteriores)**

En este tema se proporciona una lista de filtros predefinidos que se incluyeron en AppScan Source Versión 8.7.x y anteriores.

Si necesita acceder a estos filtros, siga las instrucciones en “Restauración de filtros predefinidos archivados” en la página 161.

## **! - Los pocos vitales**

Este filtro compara resultados procedentes de algunas de las categorías de vulnerabilidad más peligrosas. Solo se incluyen los resultados que se originan en un origen de comunicaciones de red externa. Este filtro ofrece un punto de partida muy enfocado para resultados de alto riesgo. Las categorías específicas que se incluyen en este filtro son:

```
Vulnerability.BufferOverflow
Vulnerability.BufferOverflow.FormatString
Vulnerability.PathTraversal
Vulnerability.CrossSiteScripting
Vulnerability.CrossSiteScripting.Reflected
Vulnerability.CrossSiteScripting.Stored
Vulnerability.Injection
Vulnerability.Injection.LDAP
Vulnerability.Injection.SQL
Vulnerability.Injection.OS
Vulnerability.Injection.XML
Vulnerability.Injection.XPath
```

## **Prioridad alta - Comunicaciones externas**

Este filtro compara los resultados que se originan fuera de la aplicación y en una red. Este filtro compara resultados que se originan en cualquier origen de tipo `Technology.Communications`.

## **Prioridad alta - Tipos importantes**

Este filtro contiene resultados procedentes de algunas de las categorías de vulnerabilidad más peligrosas, como `CrossSiteScripting` e `Injection.SQL`. Las categorías específicas que se incluyen en este filtro son:

```
Vulnerability.AppDOS
Vulnerability.Authentication.Credentials.Unprotected
Vulnerability.Authentication.Entity
Vulnerability.BufferOverflow
Vulnerability.BufferOverflow.FormatString
Vulnerability.CrossSiteScripting
Vulnerability.CrossSiteScripting.Reflected
Vulnerability.CrossSiteScripting.Stored
Vulnerability.Injection
Vulnerability.Injection.LDAP
Vulnerability.Injection.OS
Vulnerability.Injection.SQL
Vulnerability.Injection.XML
Vulnerability.Injection.XPath
Vulnerability.PathTraversal
```

## **Prioridad baja - Código de prueba**

Este filtro contiene resultados procedentes del código de prueba. Los tipos específicos de este filtro incluyen:

```
Vulnerability.Quality.TestCode
```

## **Ruido - Operaciones como-copia**

Este filtro contiene los resultados relacionados con operaciones como-copia. Una operación como-copia se produce cuando los datos se toman de un origen, de confianza o de no confianza, y las acciones que se realizan sobre los datos son de confianza.



Se buscan estos patrones:

```
Technology.Database --> Vulnerability.Injection.SQL  
Mechanism.SessionManagement --> Mechanism.SessionManagement  
Technology.XML, Technology.XML.DOM, Technology.XML.Schema,  
Technology.XML.XPath --> Vulnerability.AppDOS.XML,  
Vulnerability.Injection.XML
```

## Ruido - Problemas de registro

Este filtro contiene resultados relacionados con el manejo de errores. Los resultados encontrados pasan de una rutina de manejo de errores a un mecanismo de registro. Se compara este patrón:

```
Mechanism.ErrorHandling -->  
Vulnerability.Logging, Vulnerability.Logging.Forge, Vulnerability.Logging.Required
```

## Ruido - Gravedad baja

Este filtro contiene resultados con gravedad baja. Se incluyen todas las clasificaciones.

## Ruido - Origen de confianza

Este filtro contiene resultados procedentes de un origen de confianza. En este filtro únicamente se incluyen resultados que tienen a `java.lang.System.getProperty.*` como su origen.

## Restauración de filtros predefinidos archivados

Los filtros predefinidos que se proporcionaron con AppScan Source antes de la versión 8.8 se pueden volver a añadir al producto siguiendo los pasos de esta tarea. Una vez restaurado en una única máquina, se pueden gestionar de la misma manera que los filtros que pueda crear (por ejemplo, se pueden compartir con varios clientes).

## Acerca de esta tarea

Los filtros predefinidos archivados están ubicados en `<dir_datos>\archive\filters` (donde `<data_dir>` es la ubicación de los datos de programa AppScan Source, como se describe en “Instalación y ubicaciones de archivo de datos de usuario” en la página 335).

## Procedimiento

1. En `<dir_datos>\archive\filters`, localice el filtro o filtros que desee restaurar (los filtros de AppScan Source tienen la extensión de archivo `.off`).
2. Copie el filtro o filtros a `<dir_datos>\scanner_filters`.
3. Reinicie AppScan Source.

## Qué hacer a continuación

Para aprender cómo gestionar los filtros (incluidos los filtros archivados que ha restaurado), consulte “Creación y gestión de filtros en la vista Editor de filtros” en la página 163.

## Creación y gestión de filtros

AppScan Source ofrece varios métodos para crear y utilizar filtros. La vista principal para la creación de filtros, la vista Editor de filtros, proporciona un

extenso conjunto de reglas que pueden establecerse manualmente y a continuación guardarse en un filtro. La vista Editor de filtros también proporciona un mecanismo para gestionar los filtros creados, permitiéndole modificarlos o eliminarlos fácilmente. También puede filtrar la tabla de resultados utilizando vistas que ofrecen representaciones gráficas de los resultados, y a continuación guardar los filtros en la vista Editor de filtros. Cuando crea un filtro, las otras vistas se actualizan para reflejar sus propiedades.

- “Creación, gestión y aplicación de filtros en la vista Editor de filtros”
- “Filtrar desde las vistas Resumen de asesoramiento y Matriz de vulnerabilidad”
- “Creación de filtros en la vista Entradas y salidas”

## **Creación, gestión y aplicación de filtros en la vista Editor de filtros**

La vista Editor de filtros le permite crear filtros especificando reglas de filtrado. Los filtros creados en la vista Editor de filtros pueden guardarse, modificarse y eliminarse. Una vez que se haya creado un filtro en esta vista, podrá aplicarlo a través del menú desplegable en la vista. Consulte “Creación y gestión de filtros en la vista Editor de filtros” en la página 163.

En AppScan Source for Analysis, puede compartir los filtros que ha creado en el AppScan Enterprise Server, y acceder a los filtros que han compartido otras personas. En AppScan Source for Development, puede acceder a filtros compartidos si está ejecutando en el modo de servidor.

**Nota:** En AppScan Source for Development (plugin de Visual Studio), esta vista forma parte de la ventana Editar filtros.

## **Filtrar desde las vistas Resumen de asesoramiento y Matriz de vulnerabilidad**

**Nota:**

- La vista Resumen de asesoramiento no está disponible en macOS.
- En AppScan Source for Development (plugin de Visual Studio), estas vistas forman parte de la ventana Editar filtros.

Las vistas Resumen de asesoramiento y Matriz de vulnerabilidad ofrecen una representación gráfica de los resultados. En estas vistas, los resultados se agrupan de formas diferentes. Estos grupos pueden seleccionarse para filtrar la tabla de resultados de modo que muestre solamente los resultados que queden dentro del grupo o grupos seleccionados. Cualquier filtrado que realice mediante este método se reflejará automáticamente en la vista Editor de filtros, desde la cual puede guardar los valores del filtro.

## **Creación de filtros en la vista Entradas y salidas**

**Nota:** La vista Entradas y salidas no estará disponible en AppScan Source for Development (plugin de Visual Studio).

La vista Entradas y salidas proporciona la capacidad de visualizar y filtrar resultados basándose en un rastreo de la entrada (source) y la salida (sink). El filtrado que se hace en esta vista puede guardarse directamente en la vista. Cuando se crea un filtro, tiene la opción de aplicarlo de forma inmediata a los resultados de escaneo.

Consulte “Creación de filtros en la vista Entradas y salidas” en la página 167.

## Creación y gestión de filtros en la vista Editor de filtros

En esta vista, puede crear, editar, guardar, suprimir y gestionar filtros. Si está utilizando AppScan Source for Analysis, puede compartir filtros y acceder a filtros que otros hayan compartido. En AppScan Source for Development, puede acceder a filtros compartidos si está utilizando modo de servidor y ha iniciado una sesión en AppScan Enterprise Server.

### Procedimiento

1. En la “Vista Editor de filtros” en la página 332 barra de herramientas, pulse en **Nuevo**. El nombre del nuevo filtro es Sin título<-número> (donde el primer nuevo filtro sin título es Sin título y el siguiente nuevo filtro sin título es Sin título-1, y así sucesivamente).

**Nota:** En AppScan Source for Development (plugin de Visual Studio), esta vista forma parte de la ventana Editar filtros.

2. Expanda las categorías y seleccione los criterios que desee para el filtro.
3. Pulse en **Guardar** o **Guardar como**.
4. Dé un nombre al filtro y pulse en **Aceptar**. El nombre del nuevo filtro sustituye a Sin título<-número> en la lista de filtros.

### Qué hacer a continuación

Para aplicar el filtro, selecciónelo en el menú desplegable de la vista Editor de filtros.

**Nota:** Es posible que los filtros que se aplican fuera de la vista Matriz de vulnerabilidad no afecten a la vista Matriz de vulnerabilidad. El botón de la barra de herramientas **Mostrar recuentos de resultados filtrados** de la vista Matriz de vulnerabilidad se debe seleccionar para que el filtro refleje en la vista Matriz de vulnerabilidad.

Los filtros pueden gestionarse directamente en la vista Editor de filtros seleccionando el filtro de la lista y a continuación trabajando con él, o puede pulsar en **Gestionar filtros** para abrir el cuadro de diálogo Gestionar filtros, que proporciona una lista de los filtros guardados.

- **Modificar filtros:** Seleccione el filtro en la vista Editor de filtros o en el cuadro de diálogo Gestionar filtros y a continuación modifique las reglas de filtro y guarde los cambios.

**Nota:** Los filtros incorporados no se pueden modificar ni suprimir.

- **Suprimir filtros:** Seleccione el filtro en la vista Editor de filtros o en el cuadro de diálogo Gestionar filtros y a continuación pulse en **Suprimir**. En el cuadro de diálogo Gestionar filtros puede seleccionar varios filtros y pulsar en **Suprimir** para eliminarlos todos al mismo tiempo.
- **Crear un filtro a partir de otro filtro:** Puede modificar un filtro y a continuación pulsar en **Guardar como** para guardarlo bajo un nuevo nombre. Esto le permite crear un nuevo filtro a partir de los valores de un filtro ya existente. Puede hacerlo en el Editor de filtros o bien en el cuadro de diálogo Gestionar filtros.

**Consejo:** La misma acción se puede llevar a cabo abriendo un filtro y utilizando la acción **Guardar como** para guardarlo con un nombre nuevo. A continuación,

puede abrir el nuevo filtro y modificarlo. Si elige este método, puede crear un filtro nuevo a partir de uno de los filtros incorporado.

- **Revertir valores de filtro:** Si modifica las propiedades de un filtro y desea deshacer esos cambios, pulse en **Revertir** para devolver el filtro a sus valores guardados más recientemente. Esta acción puede llevarse a cabo en el Editor de filtros o bien en el cuadro de diálogo Gestionar filtros. En el cuadro de diálogo, si tiene varios filtros con cambios sin guardar, pulsar en **Revertir** hará que todos los filtros seleccionados que tengan cambios sin guardar se reviertan a sus valores guardados.
- **Compartir filtros** (solo AppScan Source for Analysis): Para crear un filtro compartido, ábralo en el editor de filtros y pulse en **Compartir filtro** en la barra de herramientas de la vista del Editor de filtros.

**Nota:** Para modificar, suprimir o crear filtros compartidos, debe tener el permiso **Gestionar filtros compartidos**. Para obtener información sobre cómo establecer permisos, consulte el manual *IBM Security AppScan Source Guía de instalación y administración*.

## Filtrar desde la vista Resumen de asesoramiento

Cuando finaliza un escaneo, los resultados de la misma pueden visualizarse en la vista Resumen de asesoramiento (esta vista se abre de forma predeterminada en la perspectiva Selección). En esta vista, puede crear un filtro a partir del diagrama de barras.

### Acerca de esta tarea

Una vez finalizado el escaneo, la “Vista Resumen de asesoramiento” en la página 331 contiene una representación gráfica de diagrama de barras de los resultados. La vista se puede refinar para visualizar los resultados por tipo de vulnerabilidad, API, proyecto o archivo. Si se seleccionan resultados agrupados en la vista Resumen de asesoramiento, la tabla de resultados cambia para mostrar únicamente los resultados que se han seleccionado en la vista Resumen de asesoramiento.

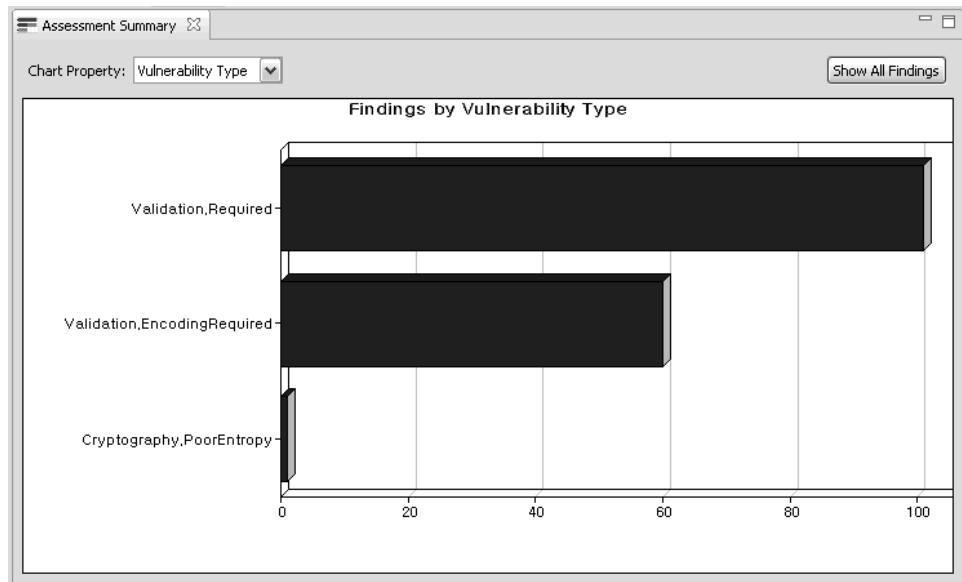
**Nota:** Es posible que los filtros que se aplican fuera de la vista Matriz de vulnerabilidad no afecten a la vista Matriz de vulnerabilidad. El botón de la barra de herramientas **Mostrar recuentos de resultados filtrados** de la vista Matriz de vulnerabilidad se debe seleccionar para que el filtro refleje en la vista Matriz de vulnerabilidad.

#### Nota:

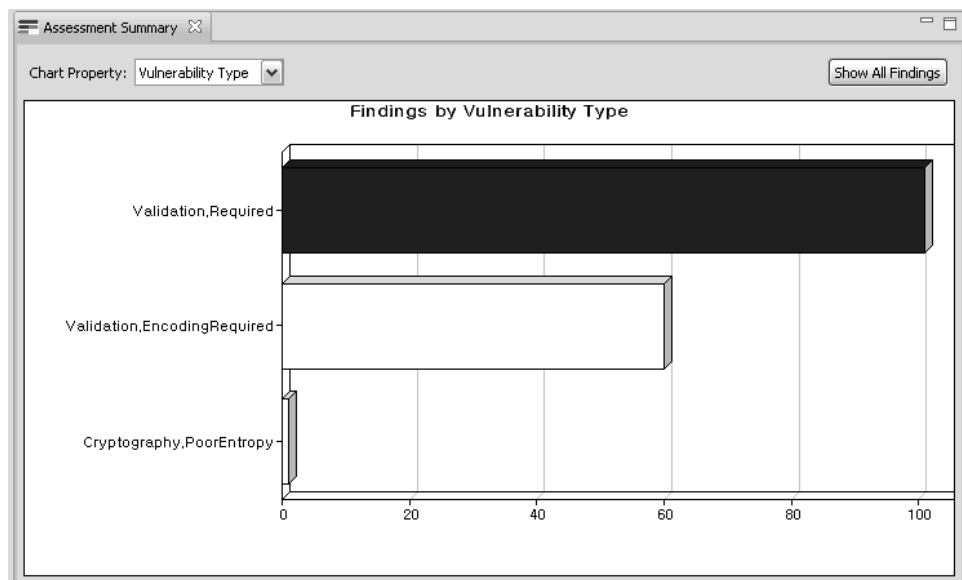
- La vista Resumen de asesoramiento no está disponible en macOS.
- En AppScan Source for Development (plugin de Visual Studio), esta vista forma parte de la ventana Editar filtros.

## Procedimiento

1. En la vista Resumen de asesoramiento, cambie la representación gráfica para adaptarla a sus necesidades. Por ejemplo, si tiene un asesoramiento que incluye los tipos de vulnerabilidad `Validation.Required`, `Validation.EncodingRequired` y `Cryptography.PoorEntropy`, establezca la **propiedad de diagrama en tipo de vulnerabilidad**. De este modo los resultados se visualizarán por tipo de vulnerabilidad en una representación de diagrama de barras:



2. Para crear un filtro de los tipos de vulnerabilidad Validation,Required, pulse la barra Validation,Required del diagrama.

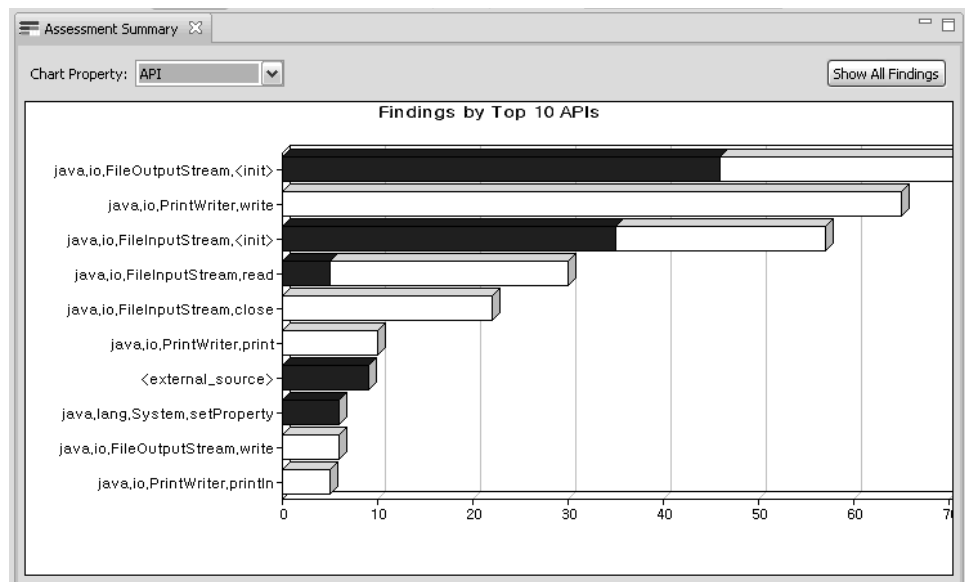


**Consejo:** Mantenga el puntero del ratón sobre la barra para ver el número de vulnerabilidades.

Los resultados filtrados aparecen en la tabla de resultados:

| Trace | Severity | Classification | Vulnerability Type   | API                   | Source             |
|-------|----------|----------------|----------------------|-----------------------|--------------------|
| ...   | High     | Suspect        | Validation, Required | java.lang.System...   | java.io.FileInp... |
| ...   | High     | Suspect        | Validation, Required | java.lang.System...   | <external_sou...   |
| ...   | High     | Suspect        | Validation, Required | java.lang.System...   | <external_sou...   |
| ...   | High     | Suspect        | Validation, Required | java.lang.System...   | <external_sou...   |
| ...   | High     | Suspect        | Validation, Required | java.lang.System...   | <external_sou...   |
| ...   | High     | Suspect        | Validation, Required | java.lang.System...   | <external_sou...   |
| ...   | Medium   | Scan Coverage  | Validation, Required | java.io.FileInputS... | java.io.FileInp... |
| ...   | Medium   | Scan Coverage  | Validation, Required | java.io.FileInputS... | java.io.FileInp... |
| ...   | Medium   | Scan Coverage  | Validation, Required | java.io.FileInputS... | java.io.FileInp... |
| ...   | Medium   | Scan Coverage  | Validation, Required | java.io.FileInputS... | java.io.FileInp... |
| ...   | Medium   | Scan Coverage  | Validation, Required | java.io.FileInputS... | java.io.FileInp... |
| ...   | Low      | Suspect        | Validation, Required | java.io.FileInputS... | <external_sou...   |
| ...   | Low      | Suspect        | Validation, Required | java.io.FileInputS... | <external_sou...   |
| ...   | Low      | Suspect        | Validation, Required | java.io.FileOutpu...  | <external_sou...   |

- Las acciones de filtrado también hacen que la vista Editor de filtros se llene con los valores de las reglas de filtro de la selección realizada en la vista Resumen de asesoramiento. Este filtro puede guardarse en la vista Editor de filtros (para obtener información acerca de los valores de las reglas de filtros y cómo guardar filtros, consulte “Creación y gestión de filtros en la vista Editor de filtros” en la página 163).
- Para ver los mismos resultados de filtro por API, establezca la **propiedad de diagrama en API**:



## Filtrar desde la vista Matriz de vulnerabilidad

La vista de la matriz de vulnerabilidad visualiza el número agregado de resultados de todas las aplicaciones incluidas en el escaneo. Estos resultados están agrupados en la matriz por nivel de gravedad. Puede crear filtros seleccionando estos grupos de resultados.

### Acerca de esta tarea

Al seleccionar resultados agrupados en “Vista Matriz de vulnerabilidad” en la página 332, la tabla de resultados cambia para mostrar únicamente los resultados seleccionados en la matriz de vulnerabilidad.

**Nota:** En AppScan Source for Development (plugin de Visual Studio), esta vista forma parte de la ventana Editar filtros.

**Nota:** Los resultados de **Calidad** y los resultados clasificados con el nivel de gravedad **Info** no se incluyen en la vista Matriz de vulnerabilidad.

### Procedimiento

1. En la vista Matriz de vulnerabilidad, seleccione la sección de la matriz que desea ver en la tabla de resultados. Por ejemplo, para ver en la tabla de resultados sólo los resultados de seguridad **sospechosos** de gravedad **alta**, seleccione dicha sección de la matriz. De este modo los resultados filtrados aparecen en la tabla de resultados.
2. Las acciones de filtrado también hacen que la vista Editor de filtros se llene con los valores de las reglas de filtro de la selección realizada en la matriz de vulnerabilidad. Este filtro puede guardarse en la vista Editor de filtros (para obtener información acerca de los valores de las reglas de filtros y cómo guardar filtros, consulte “Creación y gestión de filtros en la vista Editor de filtros” en la página 163).

## Creación de filtros en la vista Entradas y salidas

### Procedimiento

1. Abra o vaya hasta la vista Entradas y salidas.
2. La vista Entradas y salidas contiene tres secciones. La sección de la tabla de resultados de la vista muestra los resultados de las entradas, las salidas y los nodos intermedios que ha elegido mostrar en las otras dos secciones. Esto se describe en “Vista Entradas y salidas” en la página 325.
3. Una vez que haya definido la tabla de resultados para mostrar los resultados que le interesan, pulse **Crear filtro nuevo basado en la entrada, la salida y los nodos intermedios seleccionados**.
4. En el diálogo Crear filtro:
  - Especifique un nombre para el filtro en el campo **Nombre**.
  - Seleccione **Aplicar este filtro inmediatamente** para aplicar este filtro en todas las tablas de resultados de su asesoramiento. Seleccionar este recuadro de selección equivale a seleccionar un filtro en la vista Editor de filtros. Establece el filtro principal actual, que afecta a todas las vistas (por ejemplo las vistas Matriz de vulnerabilidad y Resultados).

**Nota:** Es posible que los filtros que se aplican fuera de la vista Matriz de vulnerabilidad no afecten a la vista Matriz de vulnerabilidad. El botón de la barra de herramientas **Mostrar recuentos de resultados filtrados** de la vista Matriz de vulnerabilidad se debe seleccionar para que el filtro refleje en la vista Matriz de vulnerabilidad.

- Si los resultados que se han filtrado no son relevantes para su trabajo actual, puede eliminarlos del asesoramiento seleccionando el recuadro de selección **Crear un filtro de aplicaciones que excluya estos resultados**. Al seleccionar este recuadro de selección, el nuevo filtro se añade como filtro excluido en las propiedades de la aplicación (en la vista Propiedades para la aplicación, seleccione el separador Exclusiones para ver la lista de filtros excluidos). Para futuros escaneos de la aplicación, los resultados que coincidan con el filtro se notificarán en la vista Resultados excluidos, no en la vista Resultados.
5. Pulse **Aceptar** para filtrar o excluir los resultados.

## Aplicación de filtros

Los filtros se pueden aplicar antes o después del escaneo. Para aplicar filtros después del escaneo, utilice el Editor de filtros u otra vista que le permita aplicar filtros. Para aplicar filtros antes del escaneo, establezca un filtro o un filtro global utilizando una configuración de escaneo. Al aplicar filtros antes del escaneo, no podrá mostrar resultados no filtrados ni eliminar el filtro sin escanear de nuevo.

### Aplicación de filtros antes del escaneo

Consulte “Aplicación de filtros globalmente” para obtener más información sobre cómo definir un filtro global, o “Gestión de las configuraciones de escaneo” en la página 113 para obtener más información sobre cómo establecer filtros en las configuraciones de escaneo.

### Aplicación de filtros después del escaneo

Cuando seleccione un filtro en la vista Editor de filtros, éste se aplicará automáticamente a la lista de resultados. Otras vistas proporcionan acciones de filtrado, tal como se describe en “Creación y gestión de filtros” en la página 161.

### Aplicación de filtros globalmente

Los filtros ya creados se pueden aplicar a todas las aplicaciones, a aplicaciones individuales y a proyectos individuales. Los filtros globales se aplican en la vista Propiedades, en la que se puede especificar cómo aplicarlos (un filtro se puede aplicar directamente o inversamente). Por ejemplo, si desea establecer un filtro global para una aplicación, selecciónela en la vista del explorador y abra su vista de Propiedades (utilizando el menú **Vista** o pulsando con el botón derecho del ratón en la aplicación y pulsando **Propiedades**).

### Antes de empezar

Si está estableciendo un filtro para todas las aplicaciones o para un proyecto individual, utilice el separador Filtros en la vista Propiedades. Si está estableciendo un filtro para una aplicación individual, utilice el separador Exclusiones y filtros en la vista Propiedades.

### Procedimiento

1. En la sección Filtros del separador, pulse **Añadir**.
2. En el recuadro de diálogo Seleccionar filtro, seleccione el filtro que desea aplicar globalmente.
3. Opcional: Si desea aplicar el filtro inverso (en lugar de aplicar el filtro directamente), seleccione **Invertir filtro**.
4. Pulse **Aceptar** para cerrar el recuadro de diálogo Seleccionar filtro.
5. Cuando haya terminado de añadir filtros, guardar los cambios en la vista Propiedades.

### Determinación de filtros aplicados

Los filtros se pueden aplicar de forma global a aplicaciones y proyectos antes de escanear, o bien, se pueden aplicar a los asesoramientos después del escaneo. Para permitir determinar con rapidez los filtros aplicados a los resultados en un asesoramiento, AppScan Source proporciona un indicador de filtro en la parte inferior del entorno de trabajo.



Si no se han aplicado filtros, el indicador de filtro en la parte inferior del entorno de trabajo indica que **Los resultados no están filtrados**.

Si se han aplicado filtros, el indicador cambia a un enlace que indica **Los resultados están filtrados**. Al seleccionar este enlace se abre un mensaje que permite determinar cómo se han aplicado los filtros:

- Los **Filtros de escaneo-tiempo** son filtros globales que se aplican a aplicaciones y proyectos.
  - Si el asesoramiento es el resultado de escanear una aplicación o un proyecto que no tiene configurados filtros, el mensaje indica que no se han aplicado filtros de escaneo-tiempo.
  - Si la aplicación o el proyecto que se escaneó tiene configurados filtros, los filtros configurados se listan según su nombre.
  - En la mayoría de los casos, AppScan Source detecta los filtros de escaneo-tiempo que se han aplicado, sin embargo, el asesoramiento no contiene información sobre dichos filtros. Por ejemplo, esto podría ocurrir al abrir un asesoramiento antiguo.
- Los **Filtros actuales** son filtros que se han aplicado a los resultados después del escaneo. El mensaje indica si no se han aplicado filtros actuales o si se han aplicado filtros. Si esto último ocurre, habrá disponible un enlace **restablecer**. Cuando se selecciona este enlace, los filtros actuales se eliminan de los resultados.

---

## Selección con exclusiones

Después de un escaneo, puede decidir que algunos resultados son irrelevantes para su trabajo actual, y no quiere que sean visibles en la Tabla de Resultados cuando selecciona los resultados del escaneo. Estas *exclusiones* (o resultados excluidos), dejan de aparecer en la vista Resultados y las métricas de asesoramiento se actualizan inmediatamente con los resultados modificados. Las exclusiones de filtros y paquetes añadidas a una configuración sólo tienen efecto en subsiguientes escaneos.

### El ámbito de las exclusiones

Las exclusiones se aplican a todas las aplicaciones (globales), a aplicaciones individuales o a proyectos.

- **Exclusiones globales** se aplica a todos los escaneos.
- **Exclusiones de aplicación** solo se aplican a un escaneo ejecutado para una aplicación específica y sus proyectos correspondientes.
- **Exclusiones del proyecto** se aplica a los resultados que existen en un proyecto específico.

**Nota:** Las exclusiones afectan a las métricas del asesoramiento, incluido el número total de resultados (resultados excluidos no se incluyen en las métricas del asesoramiento).

### Exclusiones globales

Puede almacenar o acceder a una exclusión global desde cualquier aplicación de AppScan Source for Analysis- y estas exclusiones se aplican a todos los escaneos. Solo los filtros compartidos se pueden convertir en filtros globales.

## Exclusiones de aplicación y de proyecto

Las exclusiones de paquete solo se aplican a una aplicación. Una exclusión de filtro se puede aplicar a una aplicación o a un proyecto. Las exclusiones que se aplican a las aplicaciones y los proyectos pueden ser compartidas o locales.

## Especificación de exclusiones

Los resultados se pueden marcar como exclusiones desde una tabla de resultados o desde la vista Propiedades. Las exclusiones pueden consistir en resultados individuales, filtros o paquetes. Generalmente, las exclusiones creadas desde una tabla de resultados entran en vigor de inmediato. Las exclusiones creadas en la vista Propiedades requieren un escaneo adicional para entrar en vigor.

Una exclusión se aplica a la aplicación de inmediato durante los siguientes procedimientos:

- Seleccionar uno o varios resultados, pulsar con el botón derecho la selección y luego seleccionar **Excluir resultados** en el menú.
- Añadir uno o varios resultados a un paquete actualmente excluido, incluido el *Paquete excluido*.
- Suprimir uno o varios resultados de un paquete previamente excluido, incluido el *Paquete excluido*.
- Suprimir un paquete excluido.

Una exclusión no se aplica a la aplicación inmediatamente cuando:

- Añadir un paquete como una exclusión.
- Añadir un filtro como una exclusión.
- Modificar un resultado para que coincida con el criterio de un filtro excluido.
- Modificar un resultado para que ya no coincida con los criterios de un filtro excluido.

## Marcar resultados como exclusiones en una tabla de resultados

### Procedimiento

1. Seleccione el resultado (o grupo de resultados) de la tabla de resultados que es posible que no considere importante o que no desee ver.
2. Pulse con el botón derecho en la selección y elija **Resultado excluido** en el menú. La exclusión o exclusiones se aplican de inmediato. Los resultados excluidos dejan de aparecer en la tabla y las métricas se actualizan inmediatamente.

### Resultados

Para visualizar resultados excluidos, abra la vista Resultados excluidos. Los resultados excluidos también aparecen en un paquete llamado **Paquete excluido**.

Para volver a incluir los resultados que se han excluido, siga las instrucciones de “Volver a incluir resultados que se han marcado como exclusiones” en la página 171.

## Volver a incluir resultados que se han marcado como exclusiones

Resultados excluidos aparecen en la vista Resultados excluidos. Desde esta vista, puede volver a incluir resultados excluidos.

### Procedimiento

1. En la vista Resultados excluidos, seleccione el resultado (o grupo de resultados) que desee volver a incluir.
2. Pulse con el botón derecho en la selección y elija **Incluir resultados** en el menú.

### Resultados

Los resultados incluidos se añaden al asesoramiento y las tablas y métricas de resultados se actualizan inmediatamente para reflejar los resultados que se han vuelto a incluir. Los resultados dejarán de aparecer en la vista de Resultados excluidos.

**Nota:** En AppScan Source for Analysis, también es posible volver a incluir resultados excluidos desde la vista de paquete **Excluidos** eliminando los resultados del paquete o moviéndolos a un nuevo paquete que no esté excluido.

## Ejemplo: Especificación de exclusiones de filtro

Los criterios de filtro determinan si el filtro excluye los resultados que coinciden o los que no coinciden con el filtro.

En estos ejemplos se describe cómo crear filtros que excluyen resultados:

- “Ejemplo: Filtrado y exclusión de un directorio”
- “Ejemplo: Filtrado y exclusión de API” en la página 172

### Ejemplo: Filtrado y exclusión de un directorio

En este ejemplo, se crea un filtro que solo muestra los resultados que contienen archivos include de Microsoft. Luego este filtro se utiliza para reducir la lista de resultados (se excluirán todos los resultados que coincidan con el filtro).

### Procedimiento

1. En la sección **Directorio** del Editor de filtros, añada la vía de acceso a los archivos de inclusión de Microsoft, (por ejemplo C:\Archivos de programa\Microsoft Visual Studio 8\VC\include).
2. Seleccione **Restringido para** para hacer que esta sea una regla de incluyente.
3. En la barra de herramientas de la vista Resultados, pulse **Mostrar resultados que no coincidan con el filtro** para ver únicamente los resultados correspondientes a archivos de cabecera de Microsoft. Esto permite ver cómo serán los resultados de escaneo después de aplicar la inversión del filtro globalmente y escanear de nuevo.
4. Guarde el filtro con un nombre, como por ejemplo **MS Includes**.
5. Vuelva a la perspectiva Configuración y, en la vista Explorador, seleccione la aplicación C/C++ o proyecto.
6. Si se selecciona una aplicación, abra el separador Exclusiones y filtros de la vista Propiedades. Si se selecciona un proyecto, abra el separador Filtros en la vista Propiedades. Pulse **Añadir**. Seleccione **MS Includes** y luego seleccione **Invertir filtro**.

7. Guarde los cambios en la vista Propiedades y, a continuación vuelva a escanear la aplicación o el proyecto de nuevo.
8. Vuelva a Selección. Los resultados de la exclusión aparecen en la vista Resultados excluidos.

### Ejemplo: Filtrado y exclusión de API

En una fase temprana del proceso de selección puede producirse un escenario de selección común, en el que desea establecer prioridad para los resultados y hay ciertos resultados que desea excluir. Por ejemplo, determina que tres API no constituyen amenazas y desea excluirlas de futuros escaneos.

#### Procedimiento

1. En el Editor de filtros, en la sección API, pulse **Añadir** y seleccione las tres API.
2. Seleccione **Restringido para**.
3. Guarde y asigne un nombre al filtro.
4. Vuelva a la perspectiva Configuración y, en la vista Explorador, seleccione el proyecto (o aplicación).
5. En la vista Propiedades, establezca el comportamiento del filtro en **Invertido** (en el recuadro de diálogo Seleccionar filtro, seleccione **Invertir filtro**).
6. Vuelva a realizar el escaneo. Las API del filtro ya no aparecen en los resultados.

#### Resultados

Siguiendo con el mismo ejemplo, supongamos que solo desea ver los resultados incluidos en el filtro. En esta instancia, al añadir el filtro a la lista, no seleccione **Invertir filtro**. Cuando vuelva a escanear, solo aparecerán los resultados del filtro.

## Especificación de exclusiones de paquetes desde la vista Propiedades

Una exclusión de paquete elimina los resultados del paquete. Solo puede excluir paquetes de las aplicaciones.

#### Procedimiento

1. Cree un paquete tal como se describe en “Creación de paquetes” en la página 173.
2. En la vista Explorador, seleccione la aplicación que desea asociar al paquete.
3. En la vista Propiedades, seleccione el separador **Exclusiones**.
4. Pulse **Añadir paquete** y, en el cuadro de diálogo Seleccionar paquete, seleccione el paquete que contiene los resultados que desea excluir de la aplicación.
5. Pulse en **Aceptar**.
6. Vuelva a realizar el escaneo. Los resultados empaquetados ya no aparecen en la tabla de resultados.

---

## Selección con paquetes

Los paquetes, que tienen características exclusivas, pueden resultar importantes para el proceso de selección.

#### Acerca de esta tarea

- Los paquetes se pueden exportar a sistemas de seguimiento de defectos como un solo defecto o como un defecto para cada resultado del paquete.

- Los paquetes pueden ser la base de la generación del informe.
- Los paquetes se adjuntan a las aplicaciones.

**Importante:** Un resultado solo puede existir en un paquete simultáneamente. Si un resultado está en un paquete, al moverlo a un paquete diferente, se eliminará del primer paquete.

Este ejemplo muestra una selección simple con paquetes:

### Procedimiento

1. Escanee el código fuente.
2. Cree un paquete llamado **Resolve ASAP**.
3. Añada algunos resultados críticos al paquete.
4. Añada notas a los resultados del paquete.
5. Envíe el paquete o los resultados al sistema de seguimiento de defectos o envíelos por correo electrónico a otros desarrolladores.
6. Arregle los problemas.

## Creación de paquetes

Los paquetes se crean en la vista **Paquete** o en una vista que contenga una tabla de resultados. Puede añadir resultados a un paquete existente o a un paquete nuevo.

Estos temas describen cómo crear paquetes en la vista **Paquetes** y en la vista **Resultados**:

- “Creación de un nuevo paquete en la vista **Paquetes**”
- “Creación de un nuevo paquete en la vista **Resultados**”

**Nota:** Para poder crear paquetes para un asesoramiento, la aplicación se ha escaneado para crear el asesoramiento debe cargarse en AppScan Source for Analysis. Si abre un asesoramiento para una aplicación que no está cargada, las acciones de creación de paquetes no estarán disponibles.

Tras haber creado uno o varios paquetes, la acción **Ocultar resultados integrados** de la vista **Resultados** (🔒) le permite conmutar la visualización de resultados empaquetados en la vista. Esta acción oculta los resultados en todos los paquetes empaquetados que ha creado. Este valor no afecta a la visualización de resultados en paquetes excluidos. Estos resultados nunca se muestran en la vista **Resultados**.

### Creación de un nuevo paquete en la vista **Paquetes**

#### Procedimiento

1. En la vista **Paquetes**, pulse **Nuevo paquete** en la barra de herramientas.
2. Asigne un nombre al paquete y pulse **Aceptar**. El nombre del paquete aparece en la vista **Paquetes**.
3. Para añadir resultados al paquete, siga las instrucciones de “Adición de resultados a paquetes existentes” en la página 174.

### Creación de un nuevo paquete en la vista **Resultados**

#### Procedimiento

1. En la vista **Resultados**, seleccione los resultados que desea añadir al paquete.

2. Pulse con el botón derecho en la selección y elija **Añadir a paquete** > **Nuevo** en el menú.
3. Asigne un nombre al paquete y pulse **Aceptar**.

## Adición de resultados a paquetes existentes

### Acerca de esta tarea

Puede añadir resultados a un paquete desde varias vistas:

- Vista Resultados
- Vista Resultados excluidos
- Vista Resultados solucionados/modificados
- Vista Resultados que faltan
- Vista de informe
- Detalle de resultado

**Consejo:** Puede mover un resultado desde la tabla de resultados a la vista Paquetes mediante una operación de arrastrar y soltar.

Para añadir resultados a un paquete:

### Procedimiento

1. Seleccione los resultados que desea añadir al paquete.
2. Pulse con el botón derecho en la selección y elija **Añadir a paquete** > **<nombre paquete>** (esta lista contiene los cinco últimos paquetes que se han creado) o **Añadir a paquete** > **Seleccionar** en el menú.
3. Si elige **Añadir a paquete** > **Seleccionar**, elija el paquete al que desea añadir los resultados en el cuadro de diálogo Seleccionar paquete y pulse **Aceptar**.

## Cómo mover resultados entre paquetes

### Procedimiento

1. En la vista Paquetes, abra el paquete que contiene el o los resultados que desea mover.
2. Seleccione el resultado o resultados que desee mover y realice una de estas acciones:
  - Pulse **Ir al paquete** o **Ir a paquete nuevo** en la barra de herramientas de la vista. A continuación, seleccione el paquete al que desea mover el resultado o cree un paquete nuevo para el resultado.
  - Pulse con el botón derecho del ratón y pulse **Ir a paquete**. Se abre un menú que le permite seleccionar un paquete existente de una lista o cuadro de diálogo, o puede crear un paquete nuevo para mover la selección al mismo.

### Resultados

**Nota:** Los resultados que se mueven o añaden a un paquete excluido no se excluirán en el asesoramiento actual. Para marcar resultados como excluidos en el asesoramiento actual, utilice la acción **Excluir resultados**.

## Visualización de resultados en paquetes

Cuando añada resultados a un paquete, los resultados aparecen como una fila en el paquete. Si abre el paquete, verá todos los resultados que contiene.

## Acerca de esta tarea

Los resultados procedentes de varios proyectos de los paquetes pueden visualizarse de forma distinta. Un resultado de un paquete aparece en verde y en cursiva si no se ha encontrado en el escaneo más reciente.

Observe el siguiente ejemplo de la Aplicación X.

### Procedimiento

1. La Aplicación X contiene el Proyecto A y el Proyecto B.
2. Escanee la Aplicación X.
3. Cree un paquete que contenga los resultados procedentes del Proyecto A y del Proyecto B.
4. Escanee el Proyecto B. En la vista Paquetes, los resultados procedentes del Proyecto B aparecen y los resultados procedentes del Proyecto A aparecen en verde y en cursiva.

### Resultados

Un resultado resaltado en verde y en cursiva es un *resultado solucionado/que falta*. Un resultado solucionado/que falta es un resultado que está en un paquete pero no en el asesoramiento actual. Un resultado se identifica como un resultado solucionado/que falta porque se ha resuelto, se ha eliminado o no se ha escaneado el archivo de origen. En la vista Paquetes, la columna **Excluido** identifica si el paquete se ha excluido.

## Guardado de paquetes en un archivo

Puede guardar un paquete como un archivo para abrirlo en AppScan Source for Development. Un paquete también permite importar una instantánea de los resultados desde AppScan Source for Analysis a AppScan Source for Remediation.

### Procedimiento

1. Realice una de estas acciones:
  - a. En la vista Paquetes, seleccione el paquete y pulse **Guardar paquete en archivo** en la barra de herramientas.
  - b. Abra el paquete y pulse **Guardar paquete en archivo** en la barra de herramientas.
2. Seleccione el directorio en el que desea guardar el archivo de paquete.
3. Asigne un nombre al archivo del paquete (<nombre\_archivo>.ozbdl).

### Resultados

Para abrir un paquete guardado:

- En AppScan Source for Development (plug-in de Eclipse), seleccione **Análisis de seguridad > Abrir > Abrir paquete**.
- En AppScan Source for Development (plug-in de Microsoft Visual Studio), seleccione **IBM Security AppScan Source > Abrir paquete**.
- En AppScan Source for Analysis, pulse **Abrir paquete** en la barra de herramientas de la vista Paquetes.

**Consejo:** En sistemas Windows, en la vista Paquetes, pulse dos veces el archivo de paquete para abrirlo en AppScan Source for Analysis o en AppScan Source for Development.

## Envío de paquetes para el seguimiento de defectos y por correo electrónico

Los resultados de los paquetes se pueden enviar al sistema de seguimiento de defectos de la empresa o se pueden enviar por correo electrónico. Cuando haya colocado los resultados en un paquete, puede enviar estos resultados como errores para su remediación por parte del desarrollador.

### Procedimiento

1. Abra el paquete.
2. Pulse la flecha hacia abajo del botón de la barra de herramientas **Enviar paquete al rastreo de defecto** y, a continuación, seleccione su sistema de seguimiento de defectos.

**Nota:** En función de su sistema de seguimiento de defectos, es posible que desee modificar las preferencias del sistema de seguimiento de defectos antes de enviar el paquete.

Como alternativa, en la barra de herramientas de Paquete, pulse **Enviar paquete por correo electrónico** para enviar el paquete a otros usuarios (se deben configurar previamente las preferencias de correo electrónico).

3. Complete los recuadros de diálogo de configuración que se vayan abriendo. Estos varían en función del sistema de seguimiento de defectos que haya elegido, y se describen en la sección *AppScan Source for Analysis y seguimiento de defectos* de la ayuda.

## Adición de notas a paquetes

### Procedimiento

1. En la vista Paquetes, seleccione el paquete que desea anotar.
2. Pulse **Añadir notas** en la barra de herramientas de la vista Paquete o pulse con el botón derecho en la selección y elija **Añadir notas** en el menú.
3. Escriba la nota y pulse **Aceptar**.

---

## Modificar resultados

Los resultados modificados son resultados que tienen notas, o cuyos tipos de vulnerabilidad, clasificación o gravedad han cambiado. La vista Resultados modificados muestra estos resultados para la aplicación actual (la aplicación que está activa como resultado de abrir un asesoramiento para esta). En la vista Mis asesoramientos (sólo disponible en AppScan Source for Analysis), la columna **Modificado** indica si el resultado ha cambiado en el asesoramiento actual.

Las modificaciones realizadas en los resultados son inmediatas y dan lugar a la actualización de las métricas. Las modificaciones se almacenan con aplicaciones y se aplican a sus futuros escaneos.

Los resultados pueden modificarse en la vista Detalle de resultado o desde cualquier vista que contenga una tabla de resultados. La vista Detalle de resultado permite modificar resultados individuales o bien puede modificar varios resultados en la tabla de resultados.



**Nota:** Debe tener permiso de **Guardar asesoramientos** para guardar cambios después de modificar un asesoramiento.

## Realizar modificaciones desde una tabla de resultados

Puede que desee modificar los resultados a través de una tabla de resultados si va a realizar los mismos cambios en varios archivos. Si va a modificar un resultado individual, utilice una tabla de resultados o la vista Detalle de resultado.

- “Cambiar el tipo de vulnerabilidad”
- “Ascender clasificaciones de resultados”
- “Modificar la gravedad”
- “Anotaciones y atributos soportados” en la página 187

### Cambiar el tipo de vulnerabilidad

Los tipos de vulnerabilidad pueden cambiarse para resultados individuales o para un grupo de resultados.

#### Procedimiento

1. En una tabla de resultados, seleccione un resultado o grupo de resultados que desee modificar.
2. Pulse con el botón derecho sobre la selección y elija **Establecer tipo de vulnerabilidad** del menú.
3. En el cuadro de diálogo Seleccionar tipo de vulnerabilidad, seleccione el tipo de vulnerabilidad que desee y pulse **Aceptar**.

### Ascender clasificaciones de resultados

Un resultado con una clasificación de resultado de cobertura de escaneo o resultado de seguridad sospechoso se puede ascender a un resultado definitivo.

#### Procedimiento

1. En una tabla de resultados, seleccione un resultado o grupo de resultados que desee modificar.
2. Pulse con el botón derecho sobre la selección y elija **Ascender a definitivo** del menú.

### Modificar la gravedad

Seleccionar un nuevo nivel de gravedad cambia la gravedad para todos los resultados seleccionados. Por ejemplo, AppScan Source podría informar de que una API es de gravedad media, pero las políticas de su empresa la identifican como más grave. Puede modificar la gravedad para cumplir con sus requisitos, pero debe tener en cuenta que la asistencia de remediación de AppScan Source no contiene la modificación.

#### Procedimiento

1. En una tabla de resultados, seleccione un resultado o grupo de resultados que desee modificar.
2. Pulse con el botón derecho sobre la selección y elija **Establecer gravedad** del menú.
3. Seleccione **Alta**, **Media**, **Baja**, o **Info** como nuevo nivel de gravedad.

## Anotar resultados

Pueden utilizarse notas para utilizarse como recordatorios para indicar que se debe realizar una acción adicional en un resultado o informar acerca del resultado a otra persona. Puede añadir una nota a un hallazgo individual o a un grupo de resultados.

### Procedimiento

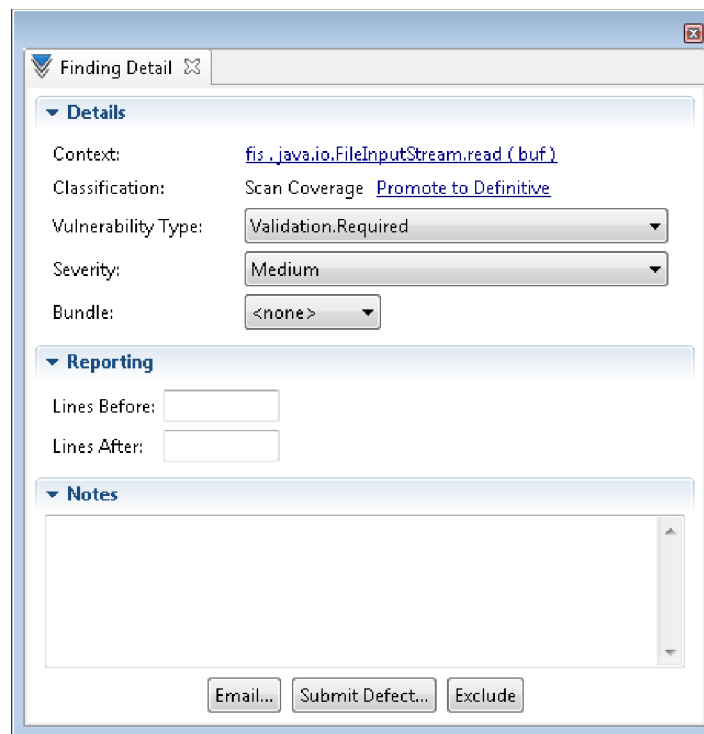
1. En una tabla de resultados, seleccione un resultado o grupo de resultados que desee modificar.
2. Pulse con el botón derecho en la selección y elija **Añadir notas** en el menú.
3. Escriba la nota y pulse **Aceptar**.

## Modificación de resultados en la vista Detalle de resultado

Pueden modificarse resultados individuales en la vista Detalle de resultado. Si selecciona un resultado de una tabla y abre la vista Detalle de resultado, aparecerá el resultado seleccionado y sus características.

### Vista Detalle de resultado

Al seleccionar un resultado, la vista Detalle de resultado muestra y le permite modificar sus propiedades. Con esta vista, puede modificar un resultado individual.



- “Sección Detalles” en la página 179
- “Sección Informes (sólo disponible en AppScan Source for Analysis y AppScan Source for Development (plugin de Eclipse))” en la página 179
- “Sección Notas” en la página 179
- “Acciones de la vista Detalles de resultados” en la página 179
- “Vista Detalles de resultados para resultados personalizados (disponible únicamente en AppScan Source for Analysis)” en la página 180

## Sección Detalles

- **Contexto:** fragmento de código que encierra la vulnerabilidad
- **Clasificación:** resultados de seguridad sospechosos o definitivos, o resultados de cobertura de escaneo, con un enlace para ascender el resultado a **Definitivo** o para volver al valor original si se cambió la clasificación.
- **Tipo de vulnerabilidad**
- **Gravedad:** alta, media, baja o informativa.
- **Paquete:** Nombre del paquete que contiene los resultados (no disponible en AppScan Source for Development (plugin de Visual Studio))

## Sección Informes (sólo disponible en AppScan Source for Analysis y AppScan Source for Development (plugin de Eclipse))

Especifique el número de líneas de código que deben incluirse en el informe antes o después del resultado.

## Sección Notas

Añadir notas al resultado.

## Acciones de la vista Detalles de resultados

- **Excluir:** Pulse en **Excluir** para excluir (eliminar) el resultado de la tabla de resultados. Para visualizar resultados excluidos, abra la vista Resultados excluidos.
- Sólo disponible en AppScan Source for Analysis:
  - **Correo electrónico:** Si ha configurado las preferencias del correo electrónico, puede enviar un resultado directamente a los desarrolladores para advertirles de potenciales defectos encontrados después de un escaneo. El correo electrónico incluye un archivo adjunto que contiene los resultados, y el texto del correo describe dichos resultados.
    1. Para enviar el resultado actual de la vista Detalle de resultado, pulse en **Correo electrónico**.
    2. En el cuadro de diálogo Nombre del archivo adjunto, especifique un nombre para el paquete de resultados que se adjuntará al correo electrónico. Por ejemplo, especificar `mi_resultado` en el campo **Nombre del archivo adjunto** hace que se adjunte al correo electrónico un paquete con el nombre de archivo `mi_resultado.ozbd1`.
    3. Pulse **Aceptar** para abrir el cuadro de diálogo Enviar resultados por correo electrónico. De forma predeterminada, el campo **Enviar a** del cuadro de diálogo Enviar resultados por correo electrónico se llenará con la **A dirección** que se especifica en las preferencias de correo electrónico. Sin embargo, se puede cambiar fácilmente al preparar el correo electrónico. En este cuadro de diálogo, revise el contenido del correo electrónico y pulse en **Aceptar** para enviar el correo electrónico.
  - **Enviar defecto:** Para enviar el resultado como defecto, pulse en **Enviar defecto**. De este modo se abrirá el cuadro de diálogo Seleccionar sistema de rastreo de defectos.
    - Si selecciona **ClearQuest** y pulsa en **Aceptar**, se abre el cuadro de diálogo Nombre del archivo adjunto. Especifique un nombre para el paquete de resultado que se adjuntará al defecto y pulse en **Aceptar**. Inicie una sesión en Rational ClearQuest y envíe los resultados.

- Si selecciona **Quality Center** y pulsa **Aceptar**, se abre el cuadro de diálogo Inicio de sesión, que le permitirá iniciar la sesión en Quality Center para enviar los resultados.
- Si selecciona la opción **Team Foundation Server**, se abre un recuadro de diálogo que le solicita que inicie la sesión en el sistema de seguimiento de defectos y proporcione otros detalles de configuración.

**Nota:** Rational Team Concert es el único sistema de seguimiento de defectos soportado en macOS.

### **Vista Detalles de resultados para resultados personalizados (disponible únicamente en AppScan Source for Analysis)**

La vista Detalle de resultado para resultados personalizados proporciona información adicional que puede editar:

- Archivo
- Línea
- Columna
- API

Además, el método mediante el cual puede editar los “Sección Detalles” en la página 179 es diferente del de los resultados estándar en algunos campos (por ejemplo, las clasificaciones para los resultados personalizados aparecen en una lista).

## **Eliminación de modificaciones de resultados**

Si ha modificado los resultados, puede eliminar las modificaciones (volver a los valores originales) utilizando los métodos que se describen en este tema.

### **Acerca de esta tarea**

Hay una variedad de métodos para eliminar las modificaciones de resultados:

- “Eliminación de modificaciones en la vista Resultados modificados” en la página 181: Este método requiere que se abra un asesoramiento para la aplicación que contenga las modificaciones que desee eliminar. Resulta útil cuando se desea revertir varios resultados modificados.
- “Eliminación de modificaciones en otras vistas con resultados” en la página 181: Este método necesita un asesoramiento abierto y es particularmente útil si ha realizado más de una modificación a un resultado y desea revertir un conjunto de cambios. Por ejemplo, si ha cambiado la gravedad y clasificación de un resultado y desea volver a la gravedad original manteniendo la clasificación modificada, este método es el más adecuado.
- “Eliminación de modificaciones en el separador Resultados modificados de la vista Propiedades (AppScan Source for Analysis solo)” en la página 181: Este método es útil si desea eliminar modificaciones para una aplicación que no tiene un asesoramiento abierto y se puede utilizar para revertir varios resultados modificados.

## Eliminación de modificaciones en la vista Resultados modificados

### Procedimiento

1. En la vista Resultados modificados, seleccione el resultado modificado que desee revertir. Se pueden seleccionar varios resultados utilizando las teclas Control y Mayúsculas en Windows - o las teclas Mandato y Mayúsculas en macOS.
2. Pulse **Suprimir modificaciones** o pulse con el botón derecho del ratón en la selección y seleccione **Suprimir modificaciones** en el menú.

### Resultados

Esta acción elimina todas las modificaciones que se han realizado en un resultado. Si ha realizado más de una modificación a un resultado y desea revertir un conjunto de cambios, utilice el método descrito en “Eliminación de modificaciones en otras vistas con resultados”.

## Eliminación de modificaciones en otras vistas con resultados Acerca de esta tarea

En cualquier vista que contenga una tabla de resultados, puede seleccionar las columnas que desea visualizar utilizando la acción **Seleccionar y ordenar columnas**. Al utilizar esta característica, puede visualizar las columnas **Gravedad (original)**, **Gravedad (personalizada)**, **Clasificación (original)** y **Clasificación (personalizada)**. Estas columnas le ayudan a devolver modificaciones a los valores originales (mediante las acciones de la tabla de resultados o utilizando la vista Detalle de resultado). Por ejemplo, un resultado con un determinado valor de **Gravedad** o **Gravedad (personalizado) Alta**, y un valor de **Gravedad (original) Media**, el nivel de gravedad puede volver a ser **Media** utilizando distintos métodos, por ejemplo:

- En una tabla de resultados, pulse con el botón derecho del ratón el resultado y seleccione **Definir gravedad > Media** en el menú.
- Seleccione el resultado y, a continuación, en la vista Detalle de resultado, establezca el campo en **Gravedad Media**.

## Eliminación de modificaciones en el separador Resultados modificados de la vista Propiedades (AppScan Source for Analysis solo)

### Procedimiento

1. En la Vista Explorador, seleccione la aplicación que contiene las modificaciones que desee eliminar.
2. En la vista Resultados modificados, seleccione el resultado modificado que desee revertir. Se pueden seleccionar varios resultados utilizando las teclas Control y Despl del teclado.
3. Pulse **Suprimir modificaciones** o pulse con el botón derecho del ratón en la selección y seleccione **Suprimir modificaciones** en el menú.

### Resultados

Esta acción elimina todas las modificaciones que se han realizado en un resultado. Si ha realizado más de una modificación a un resultado y desea revertir un conjunto de cambios, utilice el método descrito en “Eliminación de modificaciones en otras vistas con resultados”.

---

## Comparación de resultados

Los asesoramientos se comparan utilizando la acción **Diferencia entre asesoramientos**. Cuando se comparan dos asesoramientos, las diferencias entre ambos se visualizan en la vista Diferencia entre asesoramientos. Esta vista muestra los resultados nuevos, solucionados/que faltan y comunes.

Estos controles están disponibles en la vista Diferencia entre asesoramientos :

- **Diferencia entre asesoramientos**: visualizar las diferencias entre los dos asesoramientos seleccionados.
- **Nuevos resultados** (azul): utilice este botón de la barra de herramientas para conmutar la visualización de los nuevos resultados (los resultados que están en el asesoramiento con la etiqueta azul, pero no el asesoramiento con la etiqueta verde).
- **Resultados solucionados/ausentes** (verde): utilice este botón de la barra de herramientas para conmutar la visualización de los resultados solucionados/ausentes (resultados que están en el asesoramiento con la etiqueta verde, pero no en el asesoramiento con la etiqueta azul).
- **Común** (blanco): utilice este botón de la barra de herramientas para conmutar la visualización de los resultados que son comunes entre los dos asesoramientos.
- **Siguiente**: ir al siguiente bloque de resultados nuevos o solucionados/que faltan.
- **Anterior**: ir al bloque anterior de resultados nuevos o solucionados/que faltan

## Comparación de dos asesoramientos en la vista Diferencia entre asesoramientos

### Procedimiento

1. En el panel izquierdo, seleccione los dos asesoramientos que desea comparar.
2. Pulse el botón de la barra de herramientas **Diferencia entre asesoramientos** o pulse con el botón derecho en la selección y seleccione **Diferencia entre asesoramientos** en el menú.

## Comparación de dos asesoramientos en la barra del menú principal

### Procedimiento

1. Seleccione **Herramientas > Diferencia entre asesoramientos** en la barra del menú principal.
2. En el cuadro de diálogo Diferencia entre asesoramientos, seleccione dos asesoramientos.
3. Pulse **Aceptar** para abrir una comparación entre los dos asesoramientos en la vista Diferencia entre asesoramientos.

## Búsqueda de diferencias entre asesoramientos en la vista Mis asesoramientos o en vista Asesoramientos publicados

### Procedimiento

1. Seleccione dos asesoramientos en una de las vistas.
2. Pulse el botón de la barra de herramientas **Diferencia entre asesoramientos** o pulse con el botón derecho en la selección y elija **Diferencia entre**

**asesoramientos** en el menú. Se abre una comparación entre los dos asesoramientos en la vista Diferencia entre asesoramientos.

---

## Resultados personalizados

Para aumentar los resultados del análisis, puede crear *resultados personalizados*. Estos son los resultados creados por el usuario que AppScan Source for Analysis añade al asesoramiento actualmente abierto o a la aplicación seleccionada. Los resultados personalizados afectan a las métricas de asesoramiento y se pueden incluir en informes. Una vez creado, un resultado personalizado se incluye automáticamente en futuros escaneos de la aplicación.

El comportamiento de un resultado personalizado depende de la vista desde la que se ha creado.

Si se crea desde la vista Resultados, el resultado personalizado:

- Se aplica al asesoramiento actualmente abierto.
- Se guarda como parte de la aplicación y aparece en las propiedades de la aplicación.
- Afecta al escaneo actual y a futuros escaneos de la misma aplicación.
- Afecta a las métricas de asesoramiento de inmediato.

Si se crea desde la vista Propiedades o seleccionando la acción **Añadir resultado personalizado** para una aplicación seleccionada, el resultado personalizado:

- Se aplica a la aplicación seleccionada.
- Se añade al asesoramiento actual si la aplicación es la que se ha escaneado.
- Está contenido en futuros escaneos de dicha aplicación.

Si se crea desde el editor de código:

- Si hay un asesoramiento abierto, el resultado personalizado funciona como si se hubiera creado en la vista Resultados.
- Si no hay ningún asesoramiento abierto, el resultado personalizado funciona como si se hubiera creado en la vista Propiedades.

AppScan Source for Analysis guarda automáticamente la aplicación después de que se creen resultados personalizados. No puede modificar el asesoramiento sin modificar la aplicación. Sin embargo, si no hay ningún asesoramiento asociado a una aplicación, no se modifica ninguna aplicación.

Si añade resultados personalizados a una aplicación, se incluyen en futuros escaneos de dicha aplicación y no se pueden excluir. Para eliminar un resultado personalizado, debe excluirlo de un asesoramiento o suprimirlo de la aplicación.

**Nota:** Los resultados personalizados no pueden ser de tipo *solucionado/que faltan*.

Un resultado personalizado consta de estos atributos:

- **Tipo de vulnerabilidad** (necesario)
- **Gravedad** (necesario)
- **Clasificación** (necesario)
- **Archivo** (necesario)
- **Contexto**
- Número de **línea**

- Número de **columna**
- **API**
- **Notas**
- **Paquetes**

## Creación de un resultado personalizado en la vista Propiedades

La creación o edición de un resultado personalizado en la vista Propiedades de la aplicación solo afecta a resultados del asesoramiento actual y a futuros escaneos.

### Procedimiento

1. Seleccione la aplicación en la vista Explorador.
2. En la vista Propiedades, seleccione el separador **Resultados personalizados**.
3. Pulse **Crear resultado personalizado** en la barra de herramientas.
4. En el cuadro de diálogo Crear resultado personalizado, añada los elementos necesarios:

- **Tipo de vulnerabilidad**
- **Gravedad**
- **Clasificación**
- **Archivo**

Opcionalmente añada contexto, número de línea, columna, API, notas y la designación del paquete.

5. Pulse en **Aceptar** para guardar los resultados personalizados en la aplicación.



## Modificación o eliminación de un resultado personalizado en la vista Propiedades

La creación o edición de un resultado personalizado en la vista Propiedades de la aplicación solo afecta a resultados del asesoramiento actual y a futuros escaneos.

### Procedimiento

1. Seleccione el resultado. Si está eliminando los resultados personalizados, puede seleccionar un grupo de resultados para suprimirlos.
2. Para modificar la búsqueda personalizada, pulse **Editar los resultados seleccionados** en la barra de herramientas y, a continuación, modifique la información definida previamente.
3. Para eliminar el o los resultados personalizados, pulse **Suprimir los resultados seleccionados** en la barra de herramientas.

## Crear resultados personalizados en una vista de resultados

Puede crear o gestionar resultados personalizados desde varias vistas de resultados (por ejemplo, las vistas Resultados y la vista Resultados personalizados).

Cuando se crea un resultado personalizado desde una vista, se añade el nuevo resultado al asesoramiento actual y se actualizan las métricas del asesoramiento.

Cuando añada una búsqueda personalizada a una vista de resultados, pulse el botón de la barra de herramientas **Crear resultado personalizado** de la vista. Se abrirá el cuadro de diálogo Crear resultado personalizado, que deberá completar del modo en que se describe en la sección “Creación de un resultado personalizado en la vista Propiedades” en la página 184.

Para eliminar un resultado personalizado, debe excluirlo de un asesoramiento, suprimirlo de la aplicación o seguir las instrucciones en “Modificación o eliminación de un resultado personalizado en la vista Propiedades”. Estas acciones no están disponibles en las demás vistas de resultados.

## Crear resultados personalizados en el editor de código fuente

### Acerca de esta tarea

Cuando añada resultados personalizados utilizando el editor de código fuente, se aplican estas condiciones :

- Si el archivo de origen visible en el editor de código fuente pertenece al asesoramiento actualmente abierto, el resultado personalizado se añade al asesoramiento y a la aplicación asociada.
- Si el resultado personalizado no pertenece al asesoramiento actualmente abierto, el resultado personalizado solo se añade a la aplicación que contiene el archivo de origen.
- Si el archivo de origen pertenece a más de una aplicación, o si AppScan Source for Analysis no puede determinar la aplicación, debe seleccionar la aplicación adecuada.

Si crea un resultado personalizado desde el editor de código fuente, el cuadro de diálogo Crear resultado personalizado contiene información que el editor ha rellenado previamente.

- **Archivo:** nombre del archivo actualmente abierto.

- **Contexto:** cualquier texto seleccionado en el editor. Si no hay texto seleccionado, el contexto es la línea actual de la posición del cursor. Si hay varias líneas seleccionadas, todas las líneas seleccionadas constituyen el contexto.
- **Número de línea y número de columna:** el número de la línea actual y el número de columna.

Para crear un resultado personalizado desde el editor:

### Procedimiento

1. Seleccione las líneas de código que desea añadir como un resultado personalizado.
2. Pulse con el botón derecho sobre la selección y elija **Crear resultado personalizado** en el menú. El cuadro de diálogo Crear resultado personalizado se rellena con el archivo, el contexto, el número de columna y el número de línea.
3. Seleccione el **Tipo de vulnerabilidad**, la **Gravedad** y la **Clasificación**. Opcionalmente añada una API, notas, o designación del paquete.
4. Pulse en **Aceptar**.

---

## Resolución de problemas de seguridad y visualización de la asistencia de remediación

AppScan Source notifica los errores de seguridad o los fallos de diseño comunes, y ayuda en el proceso de resolución. La Base de datos de conocimientos de AppScan Source Security, así como los editores de código internos y externos, ayudan en este proceso.

### Acerca de esta tarea

La Base de datos de conocimientos de AppScan Source Security ofrece sugerencias para corregir los resultados. Esta inteligencia contextualizada para cada vulnerabilidad ofrece descripciones precisas sobre la causa de origen, gravedad del riesgo, y consejos sobre acciones para remediarla. Por ejemplo, describe, `strcpy()`, un desbordamiento de almacenamiento intermedio que tiene un nivel de gravedad alto y proporciona y proporciona esta asistencia para remediarlo:

`strcpy` es susceptible de provocar un desbordamiento del almacenamiento intermedio de destino porque no conoce la longitud de la memoria de destino y por lo tanto no puede asegurarse de que no sobrescribe una zona vecina. Debería considerar utilizar `strncpy` que toma un parámetro de longitud. `strncpy` también es un riesgo de seguridad, aunque de menos gravedad.

Para ver la Base de datos de conocimientos de AppScan Source Security:

### Procedimiento

- En AppScan Source for Analysis, abra la vista Asistencia de remediación y luego seleccione un resultado en la tabla de resultados. Se abre la vista Asistencia de remediación para dicho resultado en particular. Como alternativa, seleccione **Ayuda > Base de datos de conocimientos** en la barra del menú principal para abrir la Base de datos de conocimientos de AppScan Source Security completa en un navegador.
- En AppScan Source for Development (plugin de Eclipse), abra la vista Asistencia de remediación y seleccione un resultado en la tabla de resultados. Se abre la vista Asistencia de remediación para dicho resultado en particular.

- En AppScan Source for Development (plugin de Visual Studio), seleccione un resultado en una tabla de resultados. Seleccione **IBM Security AppScan Source > Ayuda de la base de datos conocimientos** desde el menú principal o pulse con el botón derecho del ratón sobre el resultado y seleccione **Ayuda de la base de conocimientos** desde el menú. Esta acción abre la ayuda de remediación para el resultado seleccionado.

## Análisis del código fuente en un editor

Con AppScan Source, podrá analizar o modificar código fuente en un editor interno o en distintos editores externos.

Los editores externos le permiten revisar resultados en AppScan Source for Analysis y realizar modificaciones en el código en el entorno de desarrollo que elija. Los editores externos incluyen:

*Tabla 13. Editores externos soportados*

| Editor                                                                                                        | Plataforma      |
|---------------------------------------------------------------------------------------------------------------|-----------------|
| Eclipse (consulte los requisitos del sistema AppScan Source para conocer las versiones soportadas de Eclipse) | Windows y Linux |
| Notepad                                                                                                       | Windows         |
| vi                                                                                                            | Linux           |
| Predeterminado del sistema                                                                                    | Windows y Linux |

**Nota:** No puede editar archivos de origen en un archivo WAR.

Para ver o modificar el código fuente en el editor, elija una de estas opciones:

- Realice una doble pulsación sobre un resultado de la tabla de resultados. Se abre el editor interno en la línea de código.
- Pulse con el botón derecho del ratón en un resultado de la tabla de resultados y seleccione **Abrir en editor interno** o **Abrir en editor externo > <editor>** (donde <editor> es uno de los editores externos soportados que aparecen listados en la tabla anterior).
- Seleccione un nodo de rastreo y, a continuación, seleccione el botón de la barra de herramientas **Abrir en editor interno** o **Abrir en editor externo > <editor>** o pulse el botón derecho en la selección y seleccione **Abrir en editor interno** o **Abrir en editor externo > <editor>** en el menú.

Si ha abierto un archivo en el editor, los marcadores indican las ubicaciones en el archivo que representan los resultados. Para seguirlos en sentido inverso hasta la tabla de resultados, pulse con el botón derecho la línea de código en el editor y seleccione **Mostrar en Vista de resultados** en el menú.

## Anotaciones y atributos soportados

Algunas anotaciones o atributos que se utilizan para *decorar* el código se procesan durante los escaneos. Cuando se encuentra en el código una anotación o atributo soportados durante un escaneo, la información se utiliza para marcar el método como una devolución de llamada corrupta. Un método marcado como una devolución de llamada corrupta se trata como si todos los argumentos tuviesen datos corruptos. Esto resulta en más resultados con rastreos. Las anotaciones y atributos soportados se listan en este tema de ayuda.

- “Anotaciones de Java soportadas”
- “Anotaciones de AppScan Source Java soportadas”
- “Atributos de Microsoft .NET soportados” en la página 189

## Anotaciones de Java soportadas

Tabla 14. Anotaciones de Java soportadas

| Anotación                       | Abreviatura         |
|---------------------------------|---------------------|
| javax.xml.ws.WebServiceProvider | @WebServiceProvider |
| javax.jws.WebService            | @WebService         |
| javax.jws.WebMethod             | @WebMethod          |

## Anotaciones de AppScan Source Java soportadas

- “Utilización de anotaciones de AppScan Source ”
- “@ValidatorMethod” en la página 189
- “@SuppressSecurityTrace” en la página 189
- “@CallbackMethod” en la página 189

Cuando se utiliza AppScan Source para escanear Java, se da soporte a las anotaciones a nivel de método @ValidatorMethod, @CallbackMethod y @SuppressSecurityTrace.

## Utilización de anotaciones de AppScan Source

Se pueden utilizar anotaciones siguiendo estos pasos:

1. El soporte de anotaciones está habilitado de forma predeterminado. El archivo .jar de anotaciones se encuentra en <dir\_instalación>\lib\SecurityAnnotations.jar (donde <dir\_instalación> es la ubicación de la instalación de AppScan Source).
2. Si está escaneando clases precompiladas, archivos .war, o archivos .jar, ubique el proyecto Java que contiene los fuentes anotados.
3. Añada SecurityAnnotations.jar a la vía de acceso de clases del proyecto.
4. Vuelva a generar el proyecto.

Se pueden añadir anotaciones al código fuente antes del escaneo, o bien se pueden añadir tras el escaneo y durante la selección para identificar y eliminar los falsos positivos.

Se proporcionan anotaciones para permitirle insertar sus conocimientos directamente en el código fuente en forma de anotaciones de seguridad. Puesto que las anotaciones se pueden utilizar para declarar partes de seguridad de código, se deberían utilizar con mucho cuidado. No se deben utilizar para código que se deba escanear en busca de vulnerabilidades de seguridad. Si utiliza anotaciones, un analista de seguridad puede elegir omitirlas inhabilitando la característica en <dir\_datos>\config\scanner.ozsettings (donde <data\_dir> es la ubicación de los datos de programa AppScan Source, como se describe en “Instalación y ubicaciones de archivo de datos de usuario” en la página 335). En este archivo, localice este valor:

```
<Setting
name="process_security_annotations"
value="true"
default_value="true"
```

```

description="When turned on, security annotations in the
    source code will be processed by AppScan Source."
display_name="Process Security Annotations"
type="bool"
/>

```

Para inhabilitar esta característica, cambie `value="true"` a `value="false"`.

## @ValidatorMethod

Los validadores son métodos que realizan comprobaciones en los datos de entrada y a menudo devuelven un valor booleano que indica si la entrada es o no válida. En lugar de aceptar o rechazar la entrada utilizando validadores, puede modificar la entrada del usuario a un formato aceptable. Estos métodos reciben el nombre de sanitizantes.

Utilizando la anotación `@ValidatorMethod` puede identificar todos los métodos de validador y sanitizante en el código fuente de la aplicación. Durante los escaneos de AppScan Source, esta información se utilizará para eliminar los flujos de datos que pasan a través de estos métodos, ya que los datos ahora se consideran seguros.

**Nota:** Actualmente, no hay ninguna provisión para especificar qué parámetros del método anotado se deben considerar validados. Durante los escaneos de AppScan Source, se supondrá que todos los parámetros de entrada se han validado.

## @SuppressSecurityTrace

Todos los rastreos que fluyen a través de un método marcado con esta anotación se eliminan. Esto resulta útil cuando un grupo determinado de rastreos se identifica como falsos positivos o menos importantes o interesantes que otros. Puede utilizar esta anotación para filtrar estos rastreos u ocultarlos a fin de reducir el desorden.

## @CallbackMethod

Esta anotación se utiliza para identificar devoluciones de llamada o puntos de entrada a una aplicación. Todos los argumentos se consideran corruptos.

## Atributos de Microsoft .NET soportados

Tabla 15. Atributos de Microsoft .NET soportados

| Atributo                                | Abreviatura |
|-----------------------------------------|-------------|
| System.Web.Services.WebServiceAttribute | WebService  |
| System.Web.Services.WebMethodAttribute  | WebMethod   |



---

## Capítulo 6. Rastreo de AppScan Source

Con el rastreo de AppScan Source, puede verificar si la validación de entrada y la codificación cumplen las políticas de seguridad del software. Puede consultar los resultados que producen rastreos de entrada/salida y marcar métodos como rutinas de validación y codificación, fuentes o enlaces-S, devoluciones del llamada o propagadores de datos corruptos.

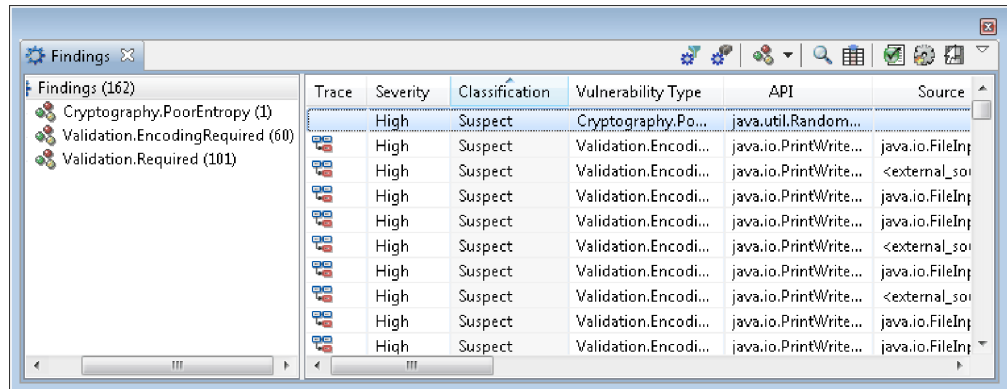
AppScan Source rastrea el flujo de datos a través de una aplicación, de módulos y de idiomas. Muestra las vías de acceso de datos potencialmente peligrosos en un gráfico de llamadas, indicando las áreas en las que la aplicación puede estar sujeta a vulnerabilidades.

El rastreo ayuda a luchar contra ataques de Inyección de SQL, scripts entre sitios y otros ataques de validación de entrada gracias a la identificación de la falta de rutinas de validación y codificación de entrada aprobadas en aplicaciones. Puede realizar el rastreo de forma interactiva de todo el gráfico de llamadas; para ello, pulse directamente en la vista Rastreo para ver el origen en el entorno de desarrollo o en el editor de código de su elección. El rastreo también permite imponer políticas, lo que permite identificar rutinas aprobadas necesarias para la correcta validación y codificación de la entrada, la propagación de datos corruptos, o las entradas y salidas, e incluirlas en futuros escaneos.

Cuando un escaneo da lugar a un rastreo, es posible crear rutinas de validación o codificación de entradas, vulnerabilidades, entradas, salidas o propagadores de datos corruptos para resultados específicos de la vista Rastreo. Por ejemplo, si marca una rutina como rutina de validación en AppScan Source for Analysis, y la añade a la Base de datos de conocimientos de AppScan Source Security, los escaneos posteriores dejarán de notificar resultados `Validation.Required` o `Validation.Encoding.Required` para las vías de acceso de datos en las que se llama a las rutinas. En la vista Rastreo también puede definir vulnerabilidades como un origen, receptor, o ambas cosas, e identificar un método como propagador corrupto, devolución de llamada corrupta, o no susceptible a la corrupción.

## Resultados de escaneo del rastreo de AppScan Source

Los resultados del escaneo pueden incluir rastreos identificados por el rastreo de AppScan Source. El icono de la columna **Rastreo** indica la existencia de un rastreo del gráfico de llamadas.



| Trace | Severity | Classification | Vulnerability Type   | API                    | Source          |
|-------|----------|----------------|----------------------|------------------------|-----------------|
|       | High     | Suspect        | Cryptography.Po...   | java.util.Random...    |                 |
|       | High     | Suspect        | Validation.Encodi... | java.io.PrintWriter... | java.io.FileInp |
|       | High     | Suspect        | Validation.Encodi... | java.io.PrintWriter... | <external_soi   |
|       | High     | Suspect        | Validation.Encodi... | java.io.PrintWriter... | java.io.FileInp |
|       | High     | Suspect        | Validation.Encodi... | java.io.PrintWriter... | java.io.FileInp |
|       | High     | Suspect        | Validation.Encodi... | java.io.PrintWriter... | <external_soi   |
|       | High     | Suspect        | Validation.Encodi... | java.io.PrintWriter... | java.io.FileInp |
|       | High     | Suspect        | Validation.Encodi... | java.io.PrintWriter... | <external_soi   |
|       | High     | Suspect        | Validation.Encodi... | java.io.PrintWriter... | java.io.FileInp |
|       | High     | Suspect        | Validation.Encodi... | java.io.PrintWriter... | java.io.FileInp |

Los escaneos pueden generar resultados de tipo `Validation.Required` y `Validation.EncodingRequired`. Estos resultados indican una ubicación en el código fuente en la que se leen datos de un origen externo o se guardan en un receptor externo. El escaneo marca estos casos porque los datos se deberían validar o codificar para evitar que datos maliciosos o erróneos produzcan daños.

## Validación y codificación

*Validación* es el proceso de comprobación de los datos de entrada para asegurarse de que tengan el formato correcto. El resultado `Validation.Required` indica que no se ha producido la validación durante el paso de los datos desde el origen hasta el receptor. La validación puede ser tan sencilla como vincular los datos a una longitud máxima y tal compleja como comprobar que los nombres y las direcciones estén bien formados. La validación también puede comprobar si hay ataques, como Inyección de SQL, detectando secuencias de caracteres no válidos que permitan dichos ataques.

*Codificación* es el proceso de transformar los datos de modo que su estado tenga el formato correcto. El resultado `Validation.EncodingRequired` indica que no se ha producido la codificación durante el paso de los datos desde el origen hasta el receptor. La codificación puede ser tan sencilla como permitir el escape de caracteres o tan compleja como cifrar los datos. La codificación también puede evitar ataques, como los de scripts entre sitios, permitiendo el escape de los caracteres que dan lugar a dichos ataques.

Cuando realiza el primer escaneo, es posible que AppScan Source identifique un resultado como un resultado de seguridad sospechoso. Cuando crea una rutina de validación o de codificación que se aplica a un origen específico, AppScan Source for Analysis notifica el resultado como definitivo (en lugar de como un resultado sospechoso) si no se llama a la rutina de validación o codificación especificada después de recibir datos procedentes del origen.

Los asesores realizan un seguimiento de los datos procedentes de orígenes conocidos durante un proyecto. Si se puede realizar el seguimiento de los datos desde un origen conocido a un receptor conocido, las rutinas de validación y

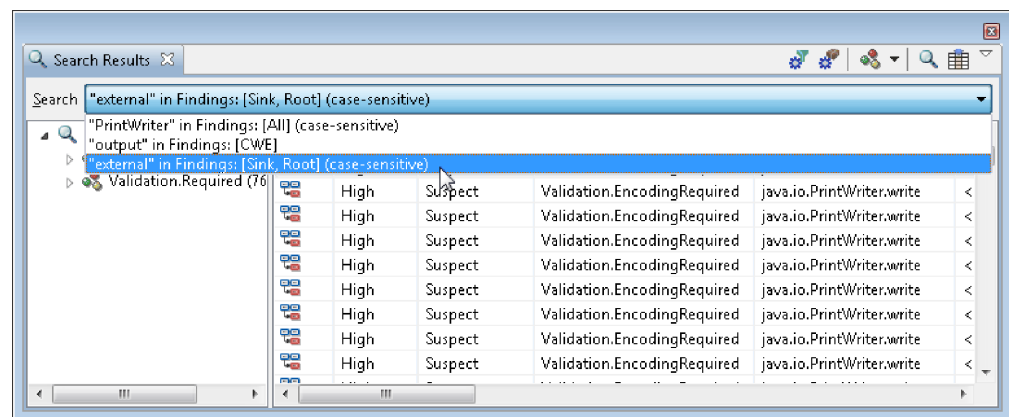


codificación especificadas pueden garantizar que no se produzca un ataque malicioso con datos de entrada no vinculados.

## Búsqueda de rastreos de AppScan Source

Si desea agrupar los resultados del rastreo, puede buscar orígenes o receptores. Esto hace que los resultados de rastreo aparezcan en la vista Resultados de la búsqueda.

En la vista Rastreo, pulse **Buscar rastreos con la misma rutina tipo**. A continuación, en el cuadro de selección Resultados de la búsqueda, seleccione origen, receptor, receptor perdido (incluye los receptores perdidos virtuales), receptor perdido virtual o llamadas de rastreo para aislar los resultados de los rastreos que contienen la serie. Los resultados de la búsqueda, que son acumulativos, se muestran en la vista Resultados de la búsqueda. Desde esta vista puede realizar otra búsqueda para refinar la búsqueda.



## Rastreo de entrada/salida

Un *rastreo de entrada/salida* se genera cuando AppScan Source for Analysis puede realizar un seguimiento de los datos desde un origen conocido a una *salida* o *salida perdida*.

### Rastreo de entrada/salida

Si el análisis de código puede realizar un seguimiento de un origen corrupto a una salida o salida perdida, el análisis produce un rastreo de entrada/salida. La raíz del rastreo es el método que obtiene datos de los orígenes que producen datos corruptos y los pasa a una serie de llamadas que finalmente graban en una salida no protegida.

### Entradas y salidas

- **Entrada:** Un origen es una entrada para el programa, como un archivo, una solicitud de servlet, una entrada de consola o un socket. En la mayoría de los orígenes de entrada, los datos devueltos son ilimitados en términos de contenido y longitud. Cuando se deselecciona una entrada, se considera que está corrupta. Las entradas se enumeran en las tablas de resultados, en la columna **Entrada**.
- **Salida:** Una salida puede tener cualquier formato externo en el que puedan escribirse datos. Como ejemplo de salida cabe citar las bases de datos, los archivos, la salida de la consola y los sockets. Escribir datos en una salida sin verificarla puede ser indicio de una grave vulnerabilidad de seguridad.

- **Salida perdida:** Una salida perdida es un método de API del que no puede realizarse el rastreo.

**Nota:** Las salidas perdidas no se aplican a los resultados encontrados de JavaScript.

## Utilización de la vista Rastreo

### Acerca de esta tarea

En la vista Rastreo puede ver un solo rastreo de entrada o salida para un resultado. El panel está dividido en tres paneles:

- Pilas de entrada y salida
- Flujo de datos
- Gráfico de llamadas gráficas

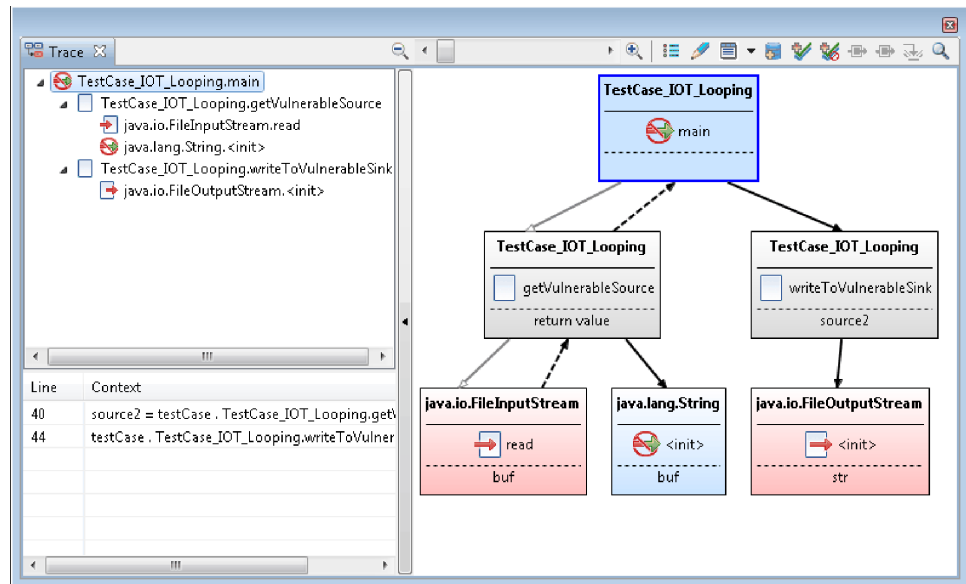
Estos paneles se describen más detalladamente en “Pilas de entrada/salida en la vista Rastreo”.

**Nota:** En un rastreo de JavaScript, en lugar de un Gráfico de llamadas gráficas se visualiza un “Gráfico de sentencias JavaScript” en la página 196.

Para ver un rastreo de AppScan Source:

### Procedimiento

1. Escanee y busque los resultados de rastreo en la ventana Resultados.
2. En el menú Ver, abra la vista Rastreo.
3. Seleccione las filas de la tabla de resultados que muestran el icono **Rastreo**. La vista Rastreo muestra los detalles del rastreo.



### Pilas de entrada/salida en la vista Rastreo

El panel superior izquierdo muestra las pilas de **entrada** y **salida**. La pila es una secuencia de llamadas que termina en un origen (pila de entrada) o en un receptor (pila de salida).

## Flujo de datos

El panel inferior izquierdo contiene el flujo de datos del método seleccionado. Los datos pueden fluir a través de una llamada de método o de una asignación. La sección flujo de datos muestra el número de línea del código fuente en el que aparecen el elemento y el contexto.

## Gráfico de llamadas

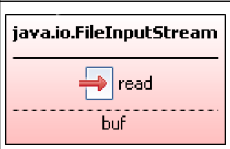
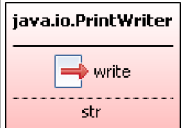
**Nota:** En un rastreo de JavaScript, en lugar de un Gráfico de llamadas gráficas se visualiza un “Gráfico de sentencias JavaScript” en la página 196.

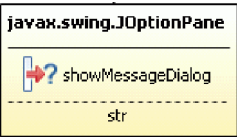
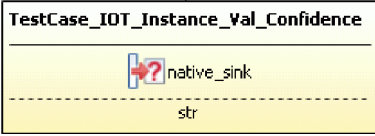
El diagrama es una representación gráfica del gráfico de llamadas. Cada llamada de método es un rectángulo dentro del gráfico que muestra el nombre de la clase y el nombre del método:

- Rojo identifica la llamada del método como un origen, un receptor o ambos.
- Un *receptor perdido* es un método de API del que ya no se puede realizar un rastreo. Un *receptor perdido virtual* es un receptor perdido que también es una función virtual (una función que puede tener más de una implementación). Amarillo identifica la llamada de método como un receptor perdido o un receptor perdido virtual.
- Azul indica la llamada de método que no es una rutina de codificación/validación.
- Gris representa los demás tipos de nodo de rastreo.

Cada llamada de método está dividida en tres secciones: el nombre de clase, el nombre de método y el nombre de argumento corrupto. Coloque el cursor sobre el texto para ver la llamada de método con más detalle.

Las líneas con flechas representan llamadas de método a método. Una punta de flecha sin relleno indica que no hay datos corruptos conocidos en la llamada, mientras que una flecha negra indica flujo de datos corruptos. Una flecha de líneas discontinuas indica una sentencia de retorno.

| Símbolo                                                                             | Descripción                                                                                                            |
|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
|  | Llamada de método sin datos corruptos conocidos                                                                        |
|  | Llamada de método con datos corruptos                                                                                  |
|  | Retorno con datos corruptos                                                                                            |
|  | Origen (rojo): un método, una función o un parámetro que es el origen de datos que probablemente no son de confianza.  |
|  | Receptor(rojo): un método o una función que probablemente es vulnerable a datos corruptos o cuyo uso supone un riesgo. |

| Símbolo                                                                           | Descripción                                                                                                                                                        |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | Receptor perdido (amarillo): un método o una función que probablemente es vulnerable a datos corruptos o cuyo uso supone un riesgo.                                |
|  | Receptor perdido virtual (amarillo): un tipo de receptor perdido que se resuelve en más de una implementación concreta.                                            |
|  | Rutina de no validación/codificación (azul). Si se marca una API como <i>rutina de no validación/codificación</i> , se indica que dicha API no valida ningún dato. |
|  | Propagador corrupto: una función o un método que propaga datos corruptos a uno o varios de sus parámetros, a su valor de retorno o a este puntero.                 |

#### Consejo:

- En la vista de rastreo, al mover el cursor sobre los nodos de rastreo en el gráfico, se proporciona información sobre el nodo.
- Los dos paneles de la izquierda en la vista (el panel de pilas de entrada/salida y el panel de flujo de datos) se pueden contraer para una mejor visualización del gráfico de llamadas gráficas. Seleccione el botón de flecha **Ocultar vista de árbol** para contraer estos paneles. Para visualizar estos paneles cuando están ocultos, seleccione el botón de flecha **Mostrar vista de árbol**.
- Mueva la barra de desplazamiento para acercarse y centrarse en los detalles, o para alejarse y tener una vista más amplia. Al pasar el ratón sobre la barra de desplazamiento de zoom se proporciona el nivel de zoom actual. Para llegar al nivel de máximo zoom, pulse **Zoom al 200%**. Para alejarse todo lo posible, pulse **Zoom para ajustar**.

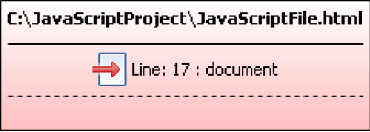
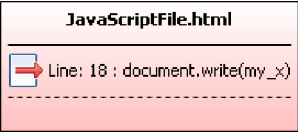
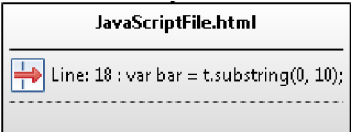
### Gráfico de sentencias JavaScript

La sección de gráfico de sentencia de un rastreo de JavaScript visualiza el flujo de datos entre sentencias.

Dentro del gráfico, cada sentencia es un rectángulo que proporciona la siguiente información:

- El nombre de archivo y la vía de acceso al archivo afectado. Si la siguiente sentencia se encuentra en el mismo archivo, únicamente se lista el nombre de archivo.
- El número de línea de la sentencia.
- Si está disponible, la sección de código que es de interés.
- Si el rectángulo es rojo, la sentencia es un origen, un receptor ("sink") o ambos.
- Si el rectángulo es gris, la sentencia es un propagador corrupto.
- Si pasa el ratón sobre el texto de la sentencia obtendrá un mayor detalle.

Las líneas con flechas representan el flujo de datos entre sentencias.

| Símbolo                                                                           | Descripción                                                                                                                              |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
|  | Flujo de datos corruptos                                                                                                                 |
|  | Origen (rojo): Una sentencia que es el origen de datos que probablemente no son de confianza.                                            |
|  | Receptor (rojo): Una sentencia que probablemente es vulnerable a datos corruptos o cuyo uso supone un riesgo.                            |
|  | Propagador corrupto: una sentencia que propaga datos corruptos a uno o varios de sus parámetros, a su valor de retorno o a este puntero. |

### Consejo:

- En la vista de rastreo, al mover el cursor sobre los nodos de rastreo en el gráfico, se proporciona información sobre el nodo.
- Los dos paneles de la izquierda en la vista (el panel de pilas de entrada/salida y el panel de flujo de datos) se pueden contraer para una mejor visualización del gráfico de llamadas gráficas. Seleccione el botón de flecha **Ocultar vista de árbol** para contraer estos paneles. Para visualizar estos paneles cuando están ocultos, seleccione el botón de flecha **Mostrar vista de árbol**.
- Mueva la barra de desplazamiento para acercarse y centrarse en los detalles, o para alejarse y tener una vista más amplia. Al pasar el ratón sobre la barra de desplazamiento de zoom se proporciona el nivel de zoom actual. Para llegar al nivel de máximo zoom, pulse **Zoom al 200%**. Para alejarse todo lo posible, pulse **Zoom para ajustar**.

## Análisis del código fuente en un editor

Con AppScan Source, podrá analizar o modificar código fuente en un editor interno o en distintos editores externos.

Los editores externos le permiten revisar resultados en AppScan Source for Analysis y realizar modificaciones en el código en el entorno de desarrollo que elija. Los editores externos incluyen:

Tabla 16. Editores externos soportados

| Editor                                                                                                        | Plataforma      |
|---------------------------------------------------------------------------------------------------------------|-----------------|
| Eclipse (consulte los requisitos del sistema AppScan Source para conocer las versiones soportadas de Eclipse) | Windows y Linux |
| Notepad                                                                                                       | Windows         |
| vi                                                                                                            | Linux           |
| Predeterminado del sistema                                                                                    | Windows y Linux |

**Nota:** No puede editar archivos de origen en un archivo WAR.

Para ver o modificar el código fuente en el editor, elija una de estas opciones:

- Realice una doble pulsación sobre un resultado de la tabla de resultados. Se abre el editor interno en la línea de código.
- Pulse con el botón derecho del ratón en un resultado de la tabla de resultados y seleccione **Abrir en editor interno** o **Abrir en editor externo > <editor>** (donde **<editor>** es uno de los editores externos soportados que aparecen listados en la tabla anterior).
- Seleccione un nodo de rastreo y, a continuación, seleccione el botón de la barra de herramientas **Abrir en editor interno** o **Abrir en editor externo > <editor>** o pulse el botón derecho en la selección y seleccione **Abrir en editor interno** o **Abrir en editor externo > <editor>** en el menú.

Si ha abierto un archivo en el editor, los marcadores indican las ubicaciones en el archivo que representan los resultados. Para seguirlos en sentido inverso hasta la tabla de resultados, pulse con el botón derecho la línea de código en el editor y seleccione **Mostrar en Vista de resultados** en el menú.

---

## Ámbito de la validación y codificación

Desde la vista Rastreo, puede especificar rutinas personalizadas de validación y codificación personalizadas que, una vez almacenadas en la Base de datos de conocimientos de AppScan Source Security, conviertan datos corruptos en datos comprobados. Con el Asistente de reglas personalizadas, puede definir estas rutinas en función de su ámbito.

Consulte el “Ejemplo 4: validación en profundidad” en la página 209 para ver el procedimiento para crear rutinas de validación y codificación.

Las rutinas de validación o codificación se basan en su ámbito y se definen como:

- “específico de API”
- “Específicas del sitio de llamada ”

### específico de API

Las rutinas de validación y codificación específicas de API se pueden asociar a un solo proyecto o a varios proyectos.

Las rutinas específicas de la API eliminarán el carácter corrupto de los datos de todas las instancias de una determinada API de origen. Por ejemplo, puede especificar una rutina de validación para cualquier entrada procedente de la API:

```
javax.servlet.ServletRequest.getParameter  
(java.lang.string):java.lang.string
```

Las rutinas específicas de la API se almacenan en el servidor. Las rutinas específicas de la API correspondientes a un proyecto se almacenan en el proyecto.

### Específicas del sitio de llamada

Las rutinas específicas del sitio de llamada siempre se asocian a un solo proyecto.

Las rutinas específicas del sitio de llamada eliminarán el carácter corrupto de los datos de una ubicación específica del código. Cuando crea una rutina de validación o codificación específica del sitio de llamada, especifica que la rutina se aplica a un determinado sitio de llamada de entrada. Las rutinas específicas del sitio de llamada siempre se almacenan en el proyecto.

**Nota:** Las rutinas específicas del sitio de llamada se aplican a cualquier llamada a la rutina de validación dentro del mismo método.

## Creación de reglas personalizadas desde un rastreo de AppScan Source

Puede crear reglas personalizadas desde la vista Rastreo que le permitan filtrar los resultados con rastreos que son propagadores corruptos, no susceptibles a la corrupción o receptores. También puede marcar métodos en el rastreo como rutinas de validación/codificación (o indicar que no son rutinas de validación/codificación).

### Acerca de esta tarea

Consulte el “Ejemplo 2: creación de una rutina de validación/codificación desde la vista Rastreo” en la página 204 para ver un ejemplo de código fuente, la salida y el procedimiento para crear las rutinas de validación y codificación.

Tabla 17. Marcas válidas para los nodos de la vista Rastreo

| Método seleccionado  | Marcas válidas                                                                                                                                                               |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nodos intermediarios | <ul style="list-style-type: none"><li>• Rutinas de validación/codificación</li><li>• No susceptible a la corrupción</li><li>• Rutina de no validación/codificación</li></ul> |
| Receptor perdido     | <ul style="list-style-type: none"><li>• Propagador corrupto</li><li>• No susceptible a la corrupción</li><li>• Receptor</li></ul>                                            |

### Procedimiento

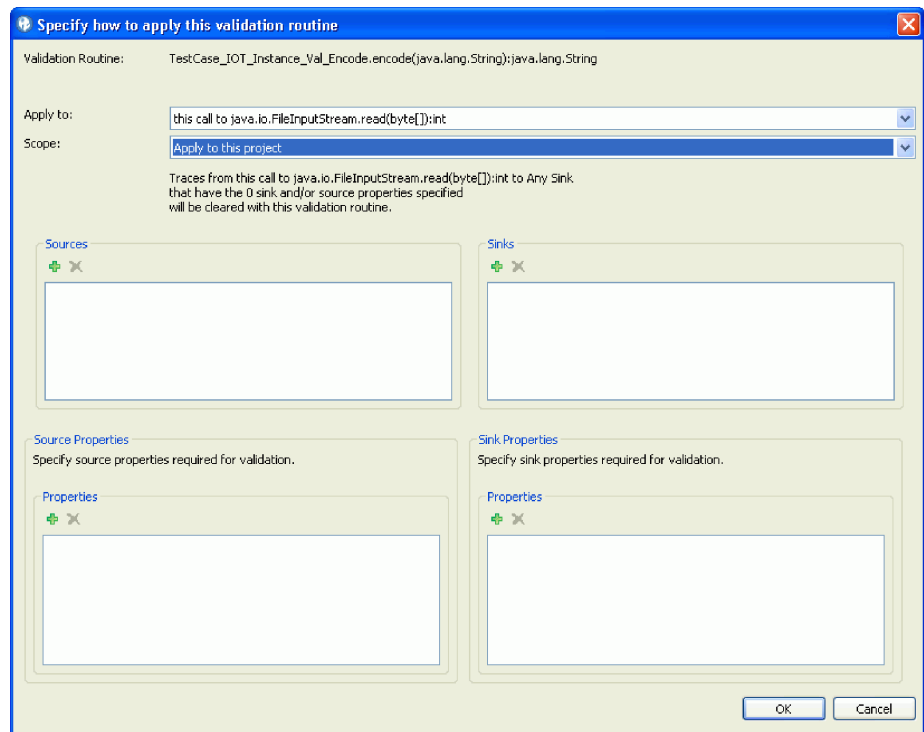
1. En la vista Rastreo, pulse con el botón derecho en el método o nodo para el cual desea crear una regla personalizada y luego elija la regla personalizada que desea crear, o bien seleccione el método o nodo y pulse el botón adecuado de la barra de herramientas de reglas personalizadas. Las opciones para marcar rutinas y métodos son:

| Opción                                           | Descripción                                                                         |
|--------------------------------------------------|-------------------------------------------------------------------------------------|
| Marcar como rutina de validación o codificación  |  |
| Marcar como rutina de no validación/codificación |  |
| Marcar como propagador corrupto                  |  |
| Marcar como no susceptible a la corrupción       |  |
| Marcar como receptor                             |  |

**Nota:** Si no existe ninguna entrada en la vista Rastreo para el método para el cual desea crear una regla personalizada, pulse **Lanzar el asistente de reglas personalizadas para añadir una rutina de validación que no se encuentra en la gráfica de rastreo**. En el asistente de reglas personalizadas, continúe en la página Seleccionar rutina de validación/codificación. Seleccione la rutina de

validación y luego especifique la ubicación, el ámbito, los orígenes o receptores, o propiedades, según las instrucciones del paso siguiente. Consulte el “Ejemplo 2: creación de una rutina de validación/codificación desde el Asistente de reglas personalizadas” en la página 207 para obtener información detallada sobre la creación de una rutina de validación con este asistente.

2. Si está creando una regla personalizada que marca un método como un receptor o una rutina de validación/codificación, puede que necesite crear valores adicionales:
  - a. Si marca el método como receptor, debe especificar los atributos del receptor:
    - **Tipo de vulnerabilidad**
    - **Gravedad**
  - b. Para rutinas de validación, especifique la ubicación y el ámbito, y los orígenes o receptores o sus propiedades, a las que deba aplicarse la rutina de validación.



- **Aplicar a:**
  - **esta llamada a <nombre método>** (específico del sitio de llamada): se aplica a la entrada solo para esta llamada.
  - **cualquier llamada <nombre método>** (específico de API): s aplica a la rutina de validación o codificación para cualquier llamada al método.
  - **<nombre de método> no se considera, a continuación se especifican todas las restricciones:** permite que esta regla afecte a todos los orígenes.
- **Ámbito:**
  - **Aplicar a este proyecto:** si se selecciona, la regla se almacena en el archivo de proyecto (.ppf).
  - **Aplicar a todos los proyectos:** las reglas de validación creadas con este valor se almacenan en la base de datos.



- **Orígenes:** seleccione el origen u orígenes de entrada a los que debe aplicarse la rutina de validación. Para añadir un origen, pulse **Añadir** y luego seleccione el origen en el cuadro de diálogo Elegir firmas. Para añadir varios orígenes, puede realizar una selección múltiple de orígenes en el cuadro de diálogo Elegir firmas.
  - **Receptores:** seleccione el receptor o receptores a los que debe aplicarse la rutina de validación. Para añadir un receptor, pulse **Añadir** y, a continuación, selecciónelo en el cuadro de diálogo Elegir firmas. Para añadir varios receptores, puede realizar una selección múltiple de receptores en el cuadro de diálogo Elegir firmas.
  - **Propiedades de origen:** si desea que la regla borre los rastreos que empiezan en un origen con una propiedad específica, pulse **Añadir una propiedad VMAT** y luego seleccione la propiedad en el cuadro de diálogo Elegir propiedades. Para añadir varias propiedades, puede realizar una selección múltiple de propiedades en el cuadro de diálogo Elegir propiedades.
  - **Propiedades de receptor:** si desea que la regla filtre los rastreos que finalizan en un receptor con una propiedad específica, pulse **Añadir una propiedad VMAT** y luego seleccione la propiedad en el cuadro de diálogo Elegir propiedades. Para añadir varias propiedades, puede realizar una selección múltiple de propiedades en el cuadro de diálogo Elegir propiedades.
3. Después de crear reglas personalizadas en la vista Rastreo, debe volver a escanear el código para ver las reglas reflejadas en las listas de resultados y rastreos. Las reglas personalizadas que crea en la vista Rastreo se pueden ver y suprimir en la vista Reglas personalizadas. Para ver detalles de la regla en la vista Reglas personalizadas, seleccione la regla y pulse **Información de reglas personalizadas**.

---

## Ejemplos de código para el rastreo

La siguiente sección proporciona ejemplos de código que muestran el seguimiento de datos corruptos desde un origen a un receptor y cómo crear una rutina de validación y codificación.

- “Ejemplo 1: desde origen a receptor”
- “Ejemplo 2: modificación entre origen y receptor” en la página 203
  - “Ejemplo 2: creación de una rutina de validación/codificación desde la vista Rastreo” en la página 204
  - “Ejemplo 2: creación de una rutina de validación/codificación desde el Asistente de reglas personalizadas” en la página 207
- “Ejemplo 3: distintos archivos de origen y de recepción” en la página 208
- “Ejemplo 4: validación en profundidad” en la página 209

### Ejemplo 1: desde origen a receptor

En el siguiente ejemplo de código, el método principal llama a un método, `getVulnerableSource`, que devuelve una serie. Tenga en cuenta que, aunque el método lee datos de un archivo completamente desconocido, nunca comprueba la validez de los datos devueltos. Luego el método principal pasa estos datos corruptos a `writeToVulnerableSink`. El método `writeToVulnerableSink` graba los datos en el archivo, sin comprobar nunca su validez.

```

import java.io.*;

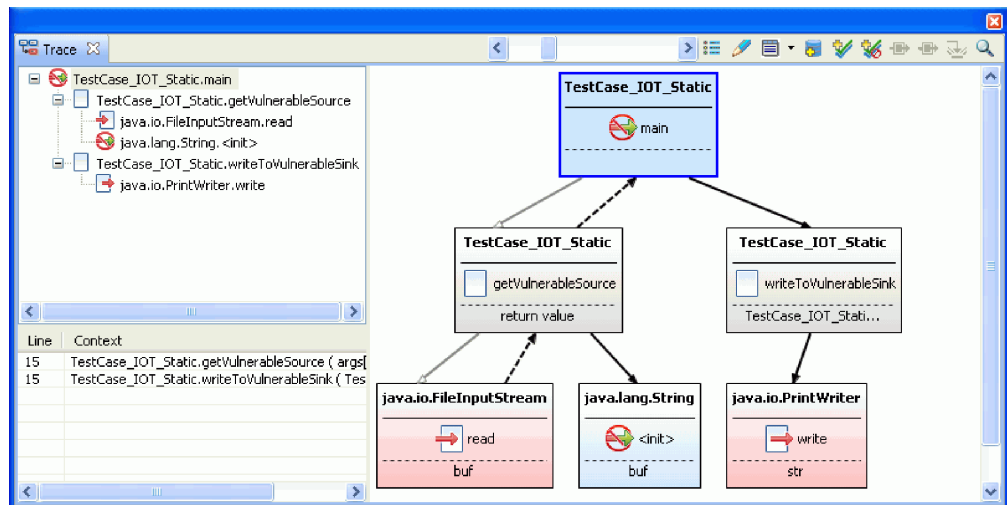
public class TestCase_IOT_Static {
    public static void main(String[] args) {
        try {
            writeToVulnerableSink(getVulnerableSource(args[0]));
        } catch (Exception e) {
        }
    }

    public static String getVulnerableSource(String file)
        throws java.io.IOException, java.io.FileNotFoundException {
        FileInputStream fis = new FileInputStream(file);
        byte[] buf = new byte[100];
        fis.read(buf);
        String ret = new String(buf);
        fis.close();
        return ret;
    }

    public static void writeToVulnerableSink(String str)
        throws java.io.FileNotFoundException {
        FileOutputStream fos = new FileOutputStream(str);
        PrintWriter writer = new PrintWriter(fos);
        writer.write(str);
    }
}

```

El ejemplo de código genera este rastreo:



El panel muestra la pila de entrada en la que main llama a getVulnerableSource, que a su vez llama a FileInputStream.read, y la pila de salida en la que main llama a writeToVulnerableSink, que a su vez llama a PrintWriter.write. El gráfico muestra cómo fluyen los datos desde el método de lectura (read) al método de grabación (write), y cómo el método principal (main) une las dos pilas de llamada. La sección Flujo de datos muestra los números de línea de las operaciones del método principal (main) que pasan los datos corruptos. En este ejemplo, ambas llamadas del método están en la misma línea (línea 15) dentro del método (en el código de ejemplo anterior, esto se convierte en la línea número 7, en la captura de pantalla, el archivo incluye 8 líneas de comentario).

## Ejemplo 2: modificación entre origen y receptor

El Ejemplo 2 es una modificación del código del Ejemplo 1. Mejora el Ejemplo 1 añadiendo una rutina de validación, denominada `getVulnerableSource`, y una rutina de codificación, denominada `writeToVulnerableSink`.

```
import java.io.*;

public class TestCase_IOT_Instance_Val_Encode {
    public static void main(String[] args) {
        try {
            TestCase_IOT_Instance_Val_Encode testCase = new
                TestCase_IOT_Instance_Val_Encode();
            String file = args[0];
            String source = testCase.getVulnerableSource(file);
            source = testCase.validate(source);
            String encodedStr = testCase.encode(source);
            testCase.writeToVulnerableSink(file, encodedStr);
        } catch (Exception e) {
        }
    }

    public String getVulnerableSource(String file) throws Exception {
        FileInputStream fis = new FileInputStream(file);
        byte[] buf = new byte[100];
        fis.read(buf);
        fis.close();

        String ret = new String(buf);
        return ret;
    }

    public void writeToVulnerableSink(String file, String str)
        throws FileNotFoundException {
        FileOutputStream fos = new FileOutputStream(file);
        PrintWriter writer = new PrintWriter(fos);
        writer.write(str);
    }

    private String validate(String source) throws Exception {
        if (source.length() > 100) {
            throw new Exception("Length too long: " + source.length());
        }
        return source;
    }

    private String encode(String source) {
        return source.trim();
    }
}
```

El primer escaneo genera un rastreo de pila parecido al del Ejemplo 1.

El hecho de ampliar la base de datos de conocimientos para incluir rutinas de validación y codificación reduce el ruido en los resultados y comprueba que se llame a las rutinas de validación y codificación para todos los gráficos de llamada. Por ejemplo, si ha especificado los datos procedentes de cualquier llamada a `java.io.FileInputStream.read(byte[]):int` en el ejemplo anterior, el escaneo elimina las llamadas procedentes de `read` que también han llamado a esta rutina de validación. Además, a las llamadas procedentes de `read` que no han llamado al método de validación se le asciende a un estado de resultado de seguridad definitivo, puesto que el hecho de no llamar a un método de validación conocido en el código puede dar lugar a ataques maliciosos.

La rutina de validación también puede validar otras variaciones de los métodos read de FileInputStream. Pueden especificarse como orígenes adicionales. Además, también puede saber que este método sólo valida determinados receptores (o receptores con determinadas propiedades). Por ejemplo, esta rutina podría estar restringida a receptores con la propiedad Technology.IO, como por ejemplo el receptor PrintWriter.write que se utiliza para consumir estos datos de ejemplo.

## Ejemplo 2: creación de una rutina de validación/codificación desde la vista Rastreo

### Acerca de esta tarea

Dado que rastreo de AppScan Source identifica el método FileInputStream.read como un origen que produce datos corruptos, debe crear una rutina de validación o de codificación para eliminar este resultado de futuros escaneos.

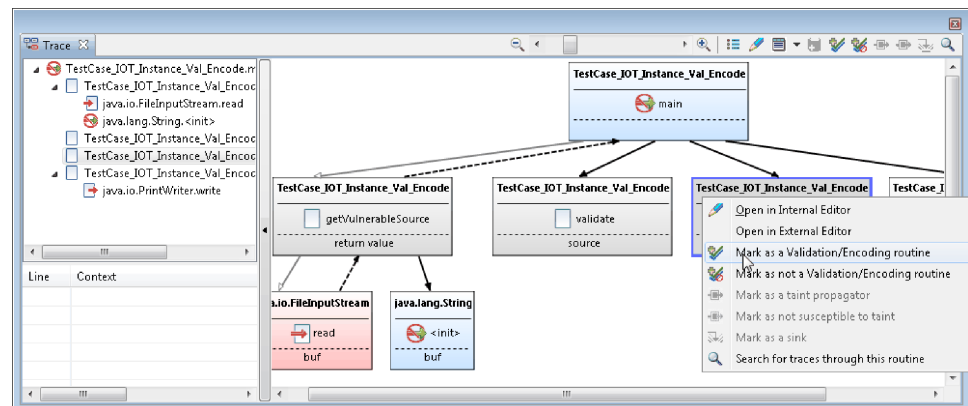
Para crear una rutina de validación de entrada para FileInputStream.read:

### Procedimiento

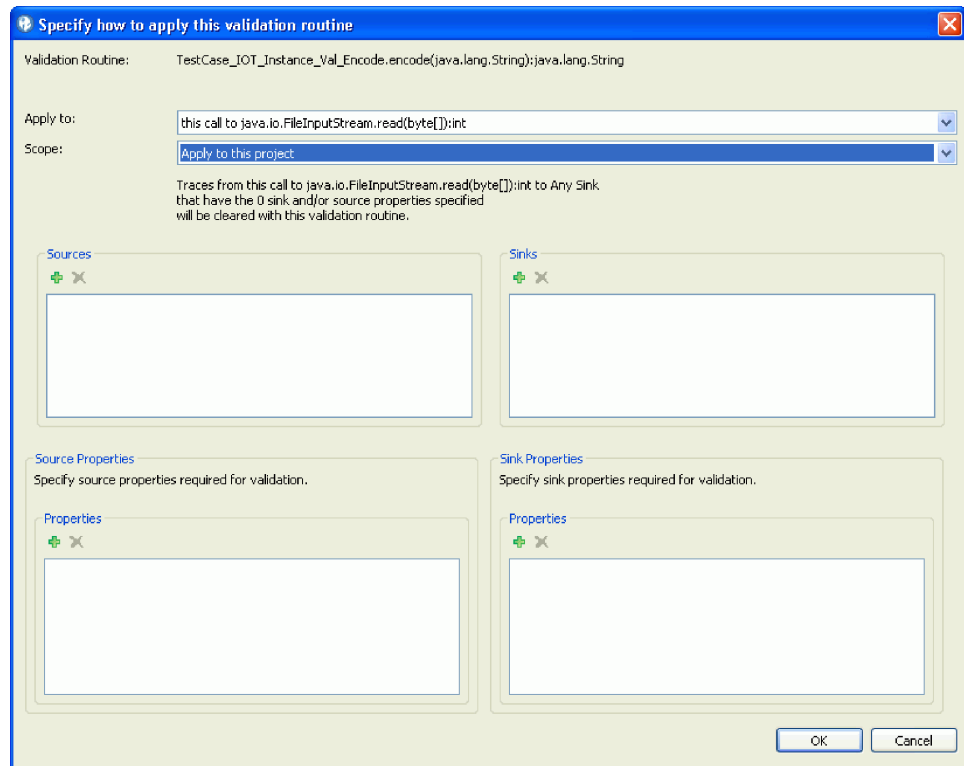
1. En el gráfico de llamadas de la vista Rastreo, seleccione y pulse con el botón derecho en el método TestCase\_IOT\_Instance\_Val\_Encode.encode.

**Consejo:** Si la rutina de validación/codificación que desea crear no aparece en la gráfica de rastreo, puede crearla iniciando el Asistente de reglas personalizadas desde la vista Rastreo. En el “Ejemplo 2: creación de una rutina de validación/codificación desde el Asistente de reglas personalizadas” en la página 207 se explican los pasos implicados en esta acción.

2. Seleccione **Marcar como rutina de validación o codificación** en el menú.



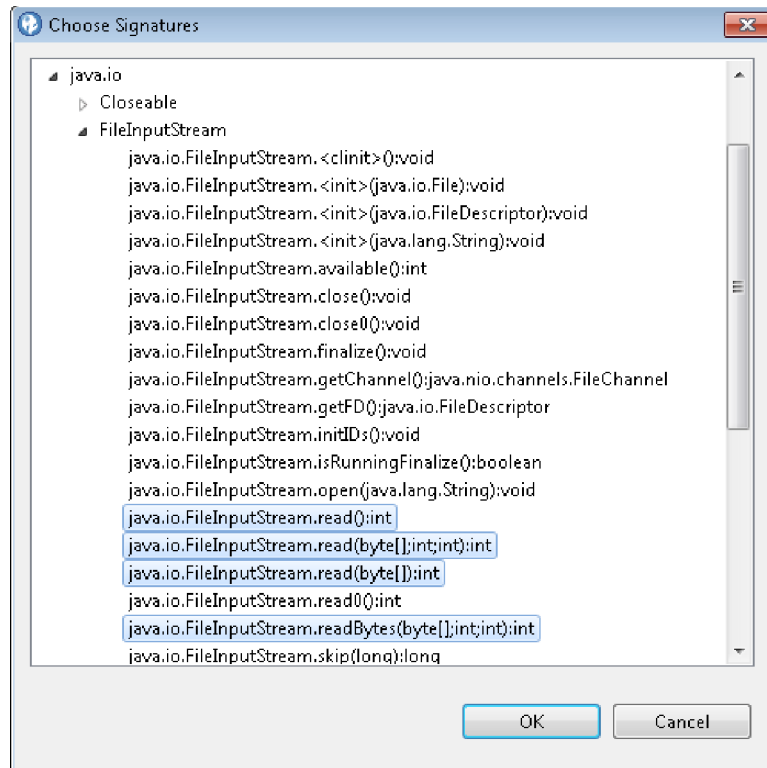
3. Se la rutina encode solo se aplica esta instancia específica de llamada a FileInputStream.read, seleccione **esta llamada a java.io.FileInputStream.read** en el cuadro de diálogo Especifique cómo aplicar esta rutina de validación.



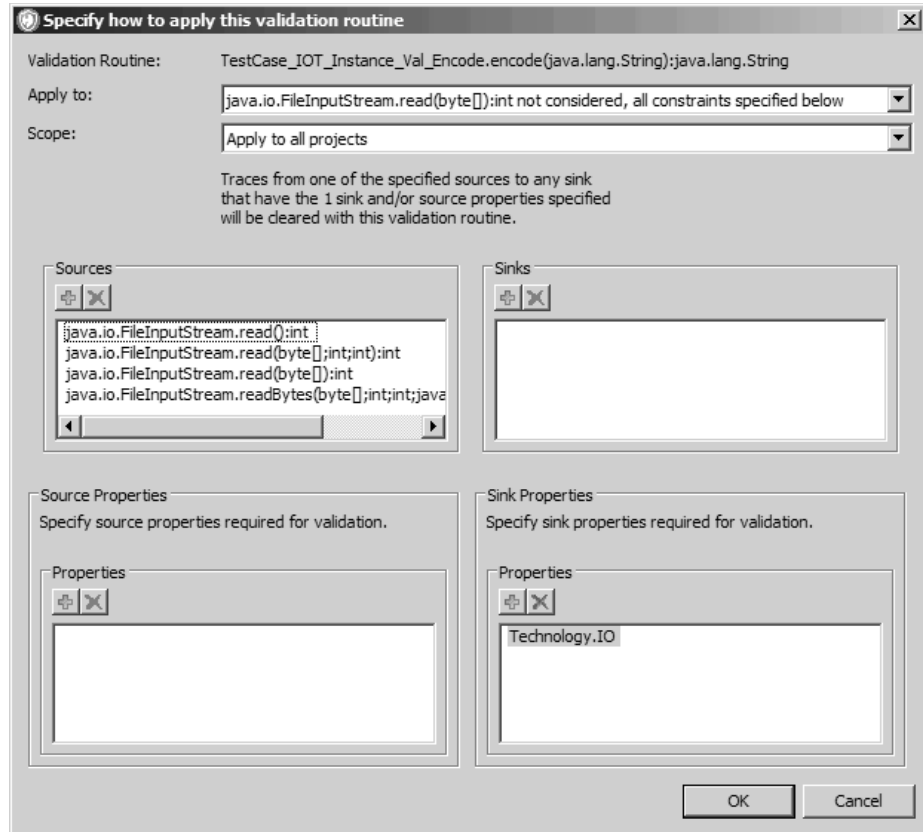
Generalmente deberá especificar **esta llamada a java.io.FileInputStream.read** porque el método validate es privado de la clase y está estrechamente asociado al código.

Seleccione **cualquier llamada a java.io.FileInputStream.read** para aplicar la rutina de validación a cualquier método read. Cuando seleccione esta opción, seleccione también **Aplicar a este proyecto** si esto solo es válido para el proyecto actual o **Aplicar a todos los proyectos**.

4. Configure la rutina para aplicarla a todos los métodos read de la clase FileInputStream y a cualquier receptor con una propiedad Technology.IO (por ejemplo, los métodos java.io.PrintWriter.write):
  - a. **Adición de los métodos read como orígenes:** Aunque podría especificar **cualquier llamada a java.io.FileInputStream.read(byte[]):int** para añadir java.io.FileInputStream.read(byte[]):int como un origen, en lugar de ello añadiremos los orígenes individualmente. En el diálogo Especifique cómo aplicar esta rutina de validación, seleccione **java.io.FileInputStream.read(byte[]):int no se considera, a continuación se especifican todas las restricciones** en el menú **Aplicar a**. A continuación pulse el botón **Añadir** de la sección **Orígenes**. En el cuadro de diálogo Elegir firmas, expanda las secciones java.io y FileInputStream. Realice una selección múltiple de los nodos java.io.FileInputStream.read\* y, después, pulse **Aceptar**.



- b. **Adición de propiedad de receptor:** pulse el botón **Añadir una propiedad VMAT** en la sección **Propiedades de receptor**. En el cuadro de diálogo **Elegir propiedades**, seleccione la propiedad **Technology.I0** y luego pulse **Aceptar**.
- c. Una vez completados todos los valores, el cuadro de diálogo debería ser similar al siguiente:



5. Pulse **Aceptar** para añadir la rutina de validación a la base de datos.

## Ejemplo 2: creación de una rutina de validación/codificación desde el Asistente de reglas personalizadas

Si la rutina de validación/codificación que desea crear no aparece en la gráfica de rastreo, puede crearla iniciando el Asistente de reglas personalizadas desde la vista Rastreo.

### Acerca de esta tarea

En este ejemplo se creará la misma rutina de validación que se crea en el “Ejemplo 2: creación de una rutina de validación/codificación desde la vista Rastreo” en la página 204; sin embargo, en este ejemplo, la rutina se creará utilizando el Asistente de reglas de personalización.

### Procedimiento

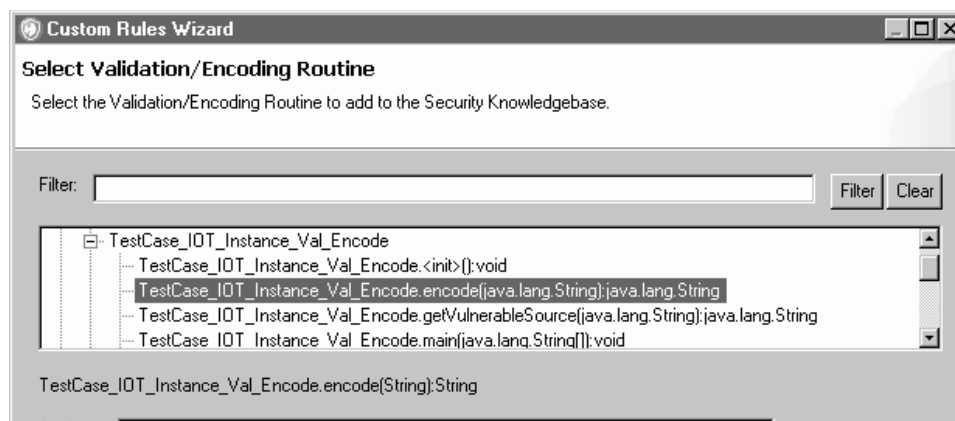
1. En la vista Rastreo, pulse **Lanzar el asistente de reglas personalizadas para añadir una rutina de validación que no se encuentra en la gráfica de rastreo** en la barra de herramientas.

**Nota:** No puede crear una rutina de validación desde el Asistente de reglas personalizadas cuando se inicia desde la vista Reglas personalizadas.

2. En la página Seleccionar rutina de validación o codificación del asistente, especifique la ubicación de la rutina de validación.

Para este ejemplo, seleccione esta rutina:

```
TestCase_IOT_Instance_Val_Encode.encode(java.lang.String):
java.lang.String
```



3. Complete las secciones restantes de la página del asistente con los mismos valores utilizados en el cuadro de diálogo **Especifique cómo aplicar esta rutina de validación** del “Ejemplo 2: creación de una rutina de validación/codificación desde la vista Rastreo” en la página 204.
4. Pulse **Finalizar** para añadir la rutina de validación a la base de datos.

### Ejemplo 3: distintos archivos de origen y de recepción

El siguiente ejemplo muestra el origen en un archivo distinto al del receptor.

#### TestCase\_IOT\_Xfile\_Part1.java:

```
public class TestCase_IOT_XFile_Part1 {
    public static void main(String[] args) {
        try {
            TestCase_IOT_XFile_Part1 testCase =
                new TestCase_IOT_XFile_Part1();
            TestCase_IOT_XFile_Part2 testCase2 =
                new TestCase_IOT_XFile_Part2();
            testCase2.writeToVulnerableSink(
                testCase.getVulnerableSource(args[0]));
        } catch (Exception e) {
        }
    }

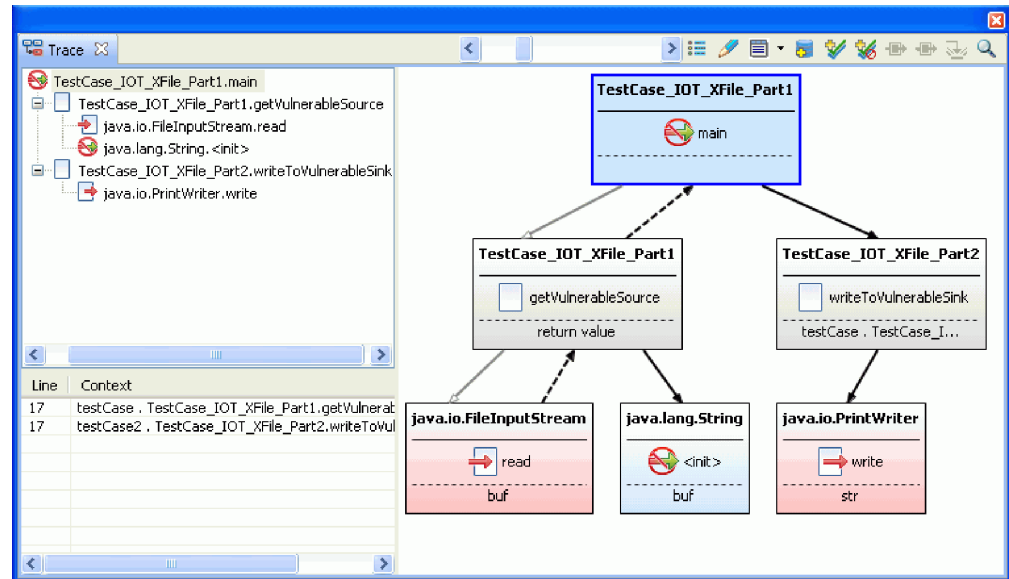
    public String getVulnerableSource(String file)
        throws IOException, FileNotFoundException {
        FileInputStream fis = new FileInputStream(file);
        byte[] buf = new byte[100];
        fis.read(buf);
        String ret = new String(buf);
        fis.close();
        return ret;
    }
}
```

#### TestCase\_IOT\_Xfile\_Part2.java:

```
public class TestCase_IOT_XFile_Part2 {
    public void writeToVulnerableSink(String str)
        throws FileNotFoundException {
        FileOutputStream fos = new FileOutputStream(str);
        PrintWriter writer = new PrintWriter(fos);
        writer.write(str);
    }
}
```



Realizar un rastreo de los datos entre TestCase\_IOT\_Xfile\_Part1.java y TestCase\_IOT\_Xfile\_Part2.java permite realizar un rastreo del flujo de datos a través de todo un programa. Aparece el rastreo de pila:



Este ejemplo muestra el flujo de datos entre TestCase\_IOT\_XFile\_Part1 y TestCase\_IOT\_XFile\_Part2 a través del método principal (main).

## Ejemplo 4: validación en profundidad

Cuando escanea el código del Ejemplo 4, el primer escaneo incluye tres rastreos de AppScan Source con una raíz en las rutinas de rastreo correspondientes. Supongamos que se ha seleccionado el método FileInputStream.read en trace1 y que se ha añadido la rutina validate. La sección que sigue al código de origen de ejemplo describe los efectos de cada ámbito para la rutina de validación.

```
public class TestCase_IOT_UserValidation {
    ResultSet resultSet;
    FileInputStream fileInputStream;
    PrintWriter printWriter;
    byte[] buffer;

    public static void main(String[] args) throws Exception {
        TestCase_IOT_UserValidation testCase = new TestCase_IOT_UserValidation();
        testCase.trace1();

        TestCase_IOT_UserValidation testCase2 = new TestCase_IOT_UserValidation();
        testCase2.trace2();

        TestCase_IOT_UserValidation testCase3 = new TestCase_IOT_UserValidation();
        testCase3.trace3();
    }

    private void trace1() throws Exception {
        String source = getVulnerableSource1();
        source = validate(source);
        writeToVulnerableSink(source);
    }

    private void trace2() throws Exception {
        String source = getVulnerableSource2();
        source = validate(source);
        writeToVulnerableSink(source);
    }
}
```

```

private void trace3() throws Exception {
    String source = getVulnerableSource3();
    source = validate(source);
    writeToVulnerableSink(source);
}

public String getVulnerableSource1() throws Exception {
    fileInputStream.read(buffer);
    return new String(buffer);
}

public String getVulnerableSource2() throws Exception {
    fileInputStream.read(buffer);
    return new String(buffer);
}

public String getVulnerableSource3() throws Exception {
    return resultSet.getString("x");
}

public void writeToVulnerableSink(String str) throws Exception {
    printWriter.write(str);
}

private String validate(String source) throws Exception {
    // validate
    return source;
}
}

```

### **Rutina de validación específica del sitio de llamada - entrada para esta llamada a `FileInputStream.read`**

Cree una rutina de validación específica del sitio de llamada cuando la validación solo se adapte a un contexto muy estrecho o cuando el método de entrada sea demasiado genérico para suministrar una rutina de validación. Cuando **aplique esta llamada a `FileInputStream.read`** en el método `trace1`, `trace1` no aparecerá como un resultado tras el siguiente escaneo porque su pila de llamada incluirá una llamada al método `validate`. Sin embargo, `trace2` sigue notificándose aunque llame a `validate`, porque el ámbito de la rutina de validación está ligado al sitio de llamada `trace1`. El método `trace3` también llama a `validate`, pero se sigue notificando porque utiliza `ResultSet.getString` como origen.

### **Rutina de validación específica de la API - entrada para cualquier llamada a `FileInputStream.read`**

Cree una rutina de validación específica de la API cuando la validación solo se pueda aplicar a un determinado origen. Cuando **aplique cualquier llamada al método `FileInputStream.read`**, los métodos `trace1` y `trace2` estarán limpios de resultados en el siguiente escaneo porque incluirán una llamada al método `validate`. Sin embargo, el método `trace3` seguirá existiendo a pesar de sus llamadas a `validate`, porque utiliza `ResultSet.getString` como origen.

---

## Capítulo 7. AppScan Source for Analysis y seguimiento de defectos

AppScan Source for Analysis se integra con sistemas de seguimiento de defectos para proporcionar vulnerabilidades de software confirmadas directamente al escritorio del desarrollador. Los defectos que se envían a un sistema de seguimiento de defectos contienen una descripción textual del defecto y un archivo que solo contiene los resultados enviados con el defecto.

Puede realizar el seguimiento de sus defectos de vulnerabilidad de software con la integración de AppScan Source for Analysis con diversos sistemas de seguimiento de defectos que incluyen IBM Rational ClearQuest, IBM Rational Team Concert, HP Quality Center y Microsoft Team Foundation Server.

Antes de enviar un resultado a un sistema de seguimiento de defectos o de enviar el defecto por correo electrónico a un desarrollador, es posible que tenga que configurar las preferencias del sistema de seguimiento de defectos (consulte “Habilitación del seguimiento de defectos con preferencias” en la página 100).

---

### Habilitación del seguimiento de defectos con preferencias

Las preferencias del sistema de seguimiento de defectos le permiten habilitar el envío de resultados a un sistema de seguimiento de defectos y determinar cómo se envían defectos.

El separador General de la página de preferencias del sistema de seguimiento de defectos sirve para habilitar o inhabilitar la característica de integración Sistema de seguimiento de defectos en AppScan Source. Si el cuadro de selección **Habilitar integración Defect Tracking System** está marcado, la acción del menú de contexto **Enviar defecto** estará disponible para los resultados de asesoramiento. El separador General también permite realizar cierto control sobre los sistemas de seguimiento de defectos que estarán disponibles cuando se envíen defectos.

Para obtener más información sobre las preferencias que se pueden definir para los sistemas de seguimiento de defectos soportados, consulte estos temas de ayuda:

- “Preferencias de Rational ClearQuest” en la página 100
- “Preferencias de Quality Center” en la página 101
- “Preferencias de Rational Team Concert” en la página 103
- “Preferencias de Team Foundation Server” en la página 104

### Preferencias de Rational ClearQuest

Para poder completar las preferencias de Rational ClearQuest, el administrador de Rational ClearQuest deberá proporcionarle los valores de Rational ClearQuest necesarios. Los valores son específicos del entorno de Rational ClearQuest.

**Nota:** Cuando se integra con Rational ClearQuest versión 8.0, el esquema Rational ClearQuest debe contener los campos disponibles en el esquema **DefectTracking** predefinido.

## **Conjunto de base de datos**

Una colección de una o varias bases de datos de defectos.

Valor predeterminado de Linux = Nombre de conexión,  
Nombre predeterminado de Windows = Conjunto de base de datos

## **Nombre de base de datos**

Nombre de la base de datos a la que se enviarán los defectos.

## **Nombre de usuario de base de datos**

Nombre de usuario de base de datos de Rational ClearQuest predeterminado.

## **Ubicación de CQPerl ejecutable**

Ubicación del archivo ejecutable de CQPerl de Rational ClearQuest en el sistema local. La ubicación predeterminada especificada se correlaciona con la ubicación de instalación de Rational ClearQuest predeterminada.

## **Entidad para registros defectuosos**

Entidad (objeto de base de datos) configurada por la instalación de Rational ClearQuest que se utilizará para objetos defectuosos.

La entidad predeterminada es **Defecto**.

## **Campo descripción en el registro**

La descripción predeterminada es **Descripción**.

## **Campo encabezamiento en el registro**

El encabezamiento predeterminado es **Encabezamiento**.

## **Defecto único por cada resultado**

Enviar un grupo de resultados como un único defecto o como varios defectos.  
Puede cambiar el método de envío cuando cree el defecto.

## **Preferencias de Quality Center**

Primero debe habilitar HP Quality Center como una preferencia general del sistema de seguimiento de defectos y luego debe establecer la preferencia individual en el separador Quality Center.

### **URL del servidor**

El URL del servidor de Quality Center, por ejemplo, `http://<hostname>:<port>/qcbn/` o `https://<hostname>:<port>/qcbn/`.

### **Nombre de usuario (opcional)**

Un nombre de usuario para iniciar una sesión en Quality Center

## **Contraseña (opcional)**

Si ha especificado un nombre de usuario, especifique la contraseña correspondiente

## **Dominio**

El dominio de Quality Center con el que va a establecer conexión.

## **Proyecto**

El proyecto de Quality Center con el que va a establecer conexión

## **Iniciar sesión automáticamente**

Cuando esta opción está habilitada, AppScan Source no solicita información de inicio de sesión al enviar resultados e inicia la sesión con las credenciales predeterminadas especificadas en las Preferencias. Si no está habilitada, debe iniciar la sesión cada vez que envíe un resultado a Quality Center.

## **Enviar automáticamente**

Cuando esta opción está habilitada, el cuadro de diálogo utilizado para enviar nuevos defectos no aparece cuando se envían resultados. AppScan Source for Analysis utiliza las **Propiedades de defecto predeterminadas** especificadas en las Preferencias. Si no está habilitada, se le solicita que especifique información sobre el defecto (Gravedad, Prioridad, Tipo de defecto, Estado, etc.) cuando envía resultados.

## **Reenvío de resultados enviados previamente**

Los resultados enviados a Quality Center se etiquetan con información sobre el defecto (ID de defecto, usuario remitente y fecha del envío). De forma predeterminada, AppScan Source no reenvía el mismo resultado más de una vez. Esto le permite asignar varios resultados a Quality Center, especificando únicamente los nuevos resultados en la base de datos de Quality Center. Cuando esta opción está seleccionada (verdadera), los resultados enviados previamente se pueden reenviar a Quality Center.

## **Envío de cada resultado como un error individual**

Cuando se envían varios resultados en una sola operación, puede enviar todos los resultados como un solo defecto de Quality Center o como un defecto de Quality Center separado para cada resultado individual de AppScan Source. Si se marca este cuadro de selección, la etiqueta se establece en verdadera, creando un defecto separado de Quality Center para cada resultado individual. Si se establece la etiqueta en falsa, se crea un defecto de Quality Center para todos los resultados enviados como parte de un envío masivo.

## **Generar automáticamente resumen de errores**

Cuando es verdadero, AppScan Source genera automáticamente un resumen de defectos para el envío a Quality Center. El resumen indica el número de resultados incluidos y el defecto y el tipo de resultados incluidos, como por ejemplo Validation.Required.

Cuando es falso, aparece el campo Resumen para que el usuario lo complete cuando envíe el defecto en el cuadro de diálogo que se abre al abrir un nuevo defecto.

## Carga automática de campos de errores

El valor predeterminado es verdadero. Cuando este cuadro de selección está marcado, AppScan Source carga automáticamente definiciones de campos de defectos de la base de datos de Quality Center, en función de los valores actuales de usuario y de grupo en Quality Center. Cuando es falso, AppScan Source no muestra campos de defectos de Quality Center en el cuadro de diálogo que se abre al abrir un nuevo defecto.

## Propiedades de defecto predeterminadas

Para establecer valores predeterminados para distintos atributos de defecto de Quality Center, pulse **Propiedades de defecto predeterminadas** en el separador de preferencias de Quality Center. Los valores predeterminados se incluyen en el cuadro de diálogo **Nuevo defecto** en el momento del envío o se envían silenciosamente a Quality Center si la preferencia **Enviar automáticamente** está seleccionada.

**Nota:** Las propiedades de defectos y sus valores disponibles se obtienen de forma dinámica de Quality Center cada vez que aparece el cuadro de diálogo **Propiedades de defecto** si **Cargar automáticamente campos de errores** está seleccionado. Por lo tanto, los nuevos campos y valores añadidos a la base de datos de Quality Center aparecen automáticamente en AppScan Source for Analysis. Se necesita información válida sobre servidor, inicio de sesión y conexión para abrir y llenar el cuadro de diálogo **Propiedades de defecto** con información de Quality Center.

## Personalización de campos de defectos de Quality Center

A través de un archivo de configuración, puede personalizar los campos y las interacciones entre dichos campos en el cuadro de diálogo Nuevo defecto. Encontrará un archivo de configuración de ejemplo en <data\_dir>\config\qc.dts (donde <data\_dir> es la ubicación de los datos de programa AppScan Source, como se describe en “Instalación y ubicaciones de archivo de datos de usuario” en la página 335), que contiene personalizaciones de ejemplo y documentación adicional. Estas personalizaciones le permiten modelar la lógica del script de flujo de trabajo de Quality Center directamente en el cuadro de diálogo Nuevo defecto.

Las personalizaciones disponibles incluyen:

- Visualizar campos personalizados, campos que faltan o ambos
- Imponer que algunos campos siempre se visualicen (modificando los valores de Quality Center)
- Actualizar el estado necesario de los campos en función de la selección de otros campos
- Actualizar dinámicamente opciones de cuadro de lista para un campo en función de la selección del cuadro de lista de otro campo

## Preferencias de Rational Team Concert

El separador Preferencias de Rational Team Concert le permite configurar una conexión con el servidor de Rational Team Concert y configurar los valores de los atributos de los elementos de trabajo.

Cuando haya especificado información sobre la conexión y haya iniciado correctamente la sesión, podrá conectar con una o varias áreas de proyecto. Cada área de proyecto puede tener su propia configuración de valores preestablecidos de atributos.

**Nota:** Al conectarse a Rational Team Concert (configurando preferencias o enviando defectos), puede que se le solicite que acepte un certificado SSL. Consulte el apartado “Certificados SSL de Rational Team Concert” en la página 104 para obtener más información.

Para configurar los valores de atributos para una determinada área de proyecto, seleccione el área de proyecto y elija **Configurar**. En el cuadro de diálogo de configuración, puede especificar valores de atributos como valores codificados y, en algunos casos, como variables que hagan referencia a un resultado seleccionado. Por ejemplo, si se usa {Finding.fileName} en un valor de atributo, se sustituirá por el nombre de archivo real del código fuente correspondiente a un resultado durante el envío. Dispone de asistencia de contenido (<Control>+<Espacio>) para los valores de atributos que dan soporte a estas variables. Se recomienda a los equipos que compartan estas configuraciones utilizando los botones **Importar** y **Exportar** disponibles en la página de preferencias principal de Rational Team Concert.

## Preferencias de Team Foundation Server

El separador Preferencias de Team Foundation Server permite configurar una conexión con un Microsoft Team Foundation Server y configurar los valores de los campos de elementos de trabajo.

Cuando haya especificado información sobre la conexión y haya iniciado correctamente la sesión, podrá conectar con uno o varios proyectos.

**Nota:** Al configurar el inicio de sesión para Team Foundation Server 2010, el URL del servidor debe contener la Recopilación de proyecto de equipo a la que se desea conectar. Por ejemplo, [http://myserver:8080/tfs/Recopilación\\_predeterminada](http://myserver:8080/tfs/Recopilación_predeterminada).

Cada proyecto puede tener su propia configuración de valores preestablecidos de campos.

Para configurar los valores de campos para un determinado proyecto, seleccione el proyecto y elija **Configurar**. En el cuadro de diálogo de configuración, puede especificar valores de campos como valores codificados y, en algunos casos, como variables que hagan referencia a un resultado seleccionado. Por ejemplo, si se usa {Finding.fileName} en un valor de campo, se sustituirá por el nombre de archivo real del código fuente correspondiente a un resultado durante el envío. Dispone de asistencia de contenido (<Control>+<Espacio>) para los campos que dan soporte a estas variables.

Se recomienda a los equipos que compartan estas configuraciones utilizando los botones **Importar** y **Exportar** disponibles en la página de preferencias principal de Team Foundation Server.

---

## Integración de HP Quality Center y AppScan Source for Analysis

Para poder integrar HP Quality Center con AppScan Source for Analysis, es necesario instalar un cliente de Quality Center en el sistema local. La aplicación cliente de Quality Center se descarga y se instala en el sistema local la primera vez que se inicia una sesión en Quality Center a través de la interfaz del cliente basada en navegador de Quality Center.

### Configuración de la información de Quality Center

Quality Center se configura en las preferencias del sistema de seguimiento de defectos, en el separador Quality Center. Debe habilitar Quality Center y establecer las preferencias de Quality Center antes de enviar resultados de AppScan Source como defectos. Consulte “Preferencias de Quality Center” en la página 101 para ver una descripción de cada uno de los valores de las preferencias.

**Nota:** En algunos entornos (por ejemplo, aquellos que ejecutan HP Quality Center Versión 11), es posible que tenga que instalar el complemento HP ALM Client MSI Generator para que la integración con HP Quality Center funcione.

### Envío de resultados a Quality Center

Los resultados se envían a Quality Center a través de cualquier vista Resultados de AppScan Source for Analysis.

#### Procedimiento

1. Seleccione uno o varios resultados de la tabla o abra un paquete. (Si abre un paquete, seleccione los resultados del paquete que desea enviar.)
2. Pulse con el botón derecho en la selección y elija **Enviar defecto > Asignar a Quality Center** en el menú.
3. Inicie una sesión en Quality Center.  
Si la preferencia está configurada para realizar un inicio de sesión automático, no aparece el cuadro de diálogo de inicio de sesión. Se inicia una sesión de AppScan Source con las credenciales predeterminadas.
4. Envíe los resultados.  
Si la preferencia está configurada para enviar automáticamente, AppScan Source envía la información de resultados utilizando las preferencias de las **Propiedades de defecto predeterminadas**.

#### Resultados

Una vez enviados los resultados, aparece un mensaje informativo que indica el número de resultados enviados correctamente.

### Seguimiento de los resultados enviados a Quality Center

Los resultados enviados a Quality Center se etiquetan con información sobre el envío:

- ID de defecto de Quality Center
- Fecha de envío
- Nombre de usuario de Quality Center

La información sobre el envío aparece en las columnas **ID de defecto**, **Fecha de defecto** y **Usuario de defecto** en una tabla de resultados de cualquier vista de



resultados. Sin embargo, la Tabla de resultados predeterminada no contiene estas columnas. Debe configurar la tabla para que incluya estas columnas pulsando el botón de la barra de herramientas **Seleccionar y ordenar columnas** y personalizando la tabla. Consulte “Personalizar la tabla de resultados” en la página 318 para ver detalles sobre cómo añadir columnas a las vistas de resultados.

La información sobre defectos se conserva de un escaneo a otro, lo que le permite realizar un seguimiento del estado de un resultado de AppScan Source durante la fase de selección y remediación.

## Información de resultados de AppScan Source en Quality Center

Cuando AppScan Source for Analysis crea un defecto en la base de datos de Quality Center, la información de resultados se establece como la **Descripción** del defecto. Esta información de resultados incluye la Gravedad, el Tipo, la API y la Clasificación.

Los defectos de Quality Center también puede contener un archivo de paquete de AppScan Source (.ozbd1) que se añade como un archivo adjunto al defecto. El archivo de paquete contiene toda la información relevante sobre el resultado de AppScan Source, incluido el rastreo. Luego los desarrolladores pueden guardar y abrir el paquete en AppScan Source for Analysis o en el plug-in Developer y realizar una selección del defecto.

---

## Integración de Rational ClearQuest y AppScan Source for Analysis

Para poder integrar Rational ClearQuest con AppScan Source for Analysis es necesario instalar un cliente de Rational ClearQuest en el sistema local. Esta instalación incluye el ejecutable de CQPer1 y el usuario debe configurar la ubicación del ejecutable en las preferencias de AppScan Source for Analysis Rational ClearQuest.

Cuando configure las preferencias de integración de Rational ClearQuest, debe especificar información sobre el esquema de la base de datos de defectos. Una entidad de Rational ClearQuest hace referencia a objetos de la base de datos de Rational ClearQuest, y el usuario debe especificar la entidad que la instalación de Rational ClearQuest utiliza para los defectos.

**Nota:** La ubicación predeterminada del ejecutable de CQPer necesario para la integración de AppScan Source for Analysis es el directorio de instalación Rational ClearQuest predeterminado.

**Nota:** Cuando se integra con Rational ClearQuest versión 8.0, el esquema Rational ClearQuest debe contener los campos disponibles en el esquema **DefectTracking** predefinido.

## Envío de resultados a Rational ClearQuest

Los resultados se integran con el sistema de seguimiento de defectos de la empresa para que el desarrollador los solucione. Puede enviar resultados individuales al sistema de rastreo de defectos, o puede enviar paquetes con uno o varios resultados. La primera vez que envía un resultado desde AppScan Source a Rational ClearQuest durante una sesión de AppScan Source, deberá iniciar la sesión con su nombre de usuario y contraseña.

Cuando envíe un paquete a Rational ClearQuest, el número de error se asocia a los resultados específicos del paquete, no al paquete propiamente dicho. Esto garantiza que pueda seguir manipulando el paquete mientras se conservan los resultados específicos asociados al defecto en el momento de creación del mismo.

Un paquete puede contener varios resultados. Tiene la opción de enviar todos los resultados como un defecto o de enviar cada resultado como un defecto separado. Si selecciona la preferencia **Defecto único por cada resultado** y hay varios resultados, puede editar la Descripción de dichos defectos. Solo puede editar la Descripción de un envío de un solo defecto.

**Nota:** Debe establecer las preferencias del sistema de seguimiento predeterminado antes de iniciar la sesión en Rational ClearQuest.

**Nota:** Cuando se integra con Rational ClearQuest versión 8.0, el esquema Rational ClearQuest debe contener los campos disponibles en el esquema **DefectTracking** predefinido.

## Envío de defectos a Rational ClearQuest

### Procedimiento

1. Seleccione uno o varios resultados de la tabla o abra un paquete. (Si abre un paquete, seleccione los resultados del paquete que desea enviar.)
2. Pulse con el botón derecho en la selección y elija **Enviar defecto > Asignar a ClearQuest** en el menú.
3. Inicie una sesión en Rational ClearQuest y envíe los resultados.

### Resultados

Se adjunta a cada defecto un archivo de asesoramiento que solo contiene los archivos relevantes. AppScan Source for Analysis o AppScan Source for Development pueden abrir este archivo de asesoramiento.

**Nota:** Cuando se integra con Rational ClearQuest versión 8.0, el esquema Rational ClearQuest debe contener los campos disponibles en el esquema **DefectTracking** predefinido.

---

## Integración de Rational Team Concert y AppScan Source for Analysis

La integración de Rational Team Concert con AppScan Source for Analysis no requiere que se instale un cliente de Rational Team Concert adicional en el sistema.

Para configurar una conexión con Rational Team Concert, vaya al separador Rational Team Concert de las preferencias del sistema de seguimiento de defectos; también puede enviar un defecto y se le solicitará que inicie una sesión y que configure la conexión.

Las preferencias de Rational Team Concert también le permiten configurar valores de campos preestablecidos que se utilizarán durante el envío de defectos. Esto le permite establecer los valores que desea utilizar para cada defecto y modificar los valores predeterminados que se suministran con AppScan Source.

**Nota:** Al conectarse a Rational Team Concert (configurando preferencias o enviando defectos), puede que se le solicite que acepte un certificado SSL. Consulte el apartado “Certificados SSL de Rational Team Concert” en la página 104 para obtener más información.

## Envío de defectos a Rational Team Concert

Puede enviar paquetes con uno o varios resultados a Rational Team Concert y también puede enviar resultados individuales. La primera vez que envíe un resultado de AppScan Source for Analysis a Rational Team Concert, deberá iniciar una sesión con su nombre de usuario y contraseña. Si desea configurar los valores de campos preestablecidos que se utilizarán durante el envío, puede hacerlo en las preferencias de Rational Team Concert.

### Acerca de esta tarea

Cuando envía un paquete a Rational Team Concert, el número del elemento de trabajo se asocia a los resultados específicos del paquete, no al paquete propiamente dicho. Esto garantiza que pueda seguir manipulando el paquete mientras se conserva la asociación de resultados específicos a números de elementos de trabajo.

### Procedimiento

1. Seleccione uno o varios resultados de la tabla o abra el paquete. (Si abre el paquete, seleccione los resultados del paquete que desea enviar.)
2. Pulse con el botón derecho en la selección y elija **Enviar defecto > Asignar a Rational Team Concert** en el menú.
3. El cuadro de diálogo de envío le guiará por el proceso, incluido el inicio de sesión, si es necesario, y la especificación de los atributos necesarios.

**Nota:** Al conectarse a Rational Team Concert (configurando preferencias o enviando defectos), puede que se le solicite que acepte un certificado SSL. Consulte el apartado “Certificados SSL de Rational Team Concert” en la página 104 para obtener más información.

### Resultados

Se añadirá automáticamente un paquete al elemento de trabajo enviado, que podrá abrir posteriormente un usuario de AppScan Source for Analysis o AppScan Source for Development

## Certificados SSL de Rational Team Concert

Cuando se instala el servidor Rational Team Concert, se debe configurar de modo que utilice un certificado SSL válido. Si no se hace, recibirá un mensaje de conexión no fiable cuando inicie la sesión en el servidor (configurando preferencias o enviando defectos). Este tema muestra las consideraciones del certificado SSL de Rational Team Concert.

### Ubicación del almacenamiento de certificados SSL

Los certificados que se han aceptado de forma permanente se guardan en `<user_home>/jazzcerts` (donde `<user_home>` es el directorio de inicio del sistema operativo (por ejemplo, en Windows, el directorio puede ser `C:\Documents and Settings\Administrator\`)). Al eliminar `<user_home>/jazzcerts` se eliminan todos

los certificados almacenados para los clientes de AppScan Source y Rational Team Concert.

### **El certificado SSL se comparte con los clientes Rational Team Concert**

AppScan Source comparte su almacén de certificados con clientes de Rational Team Concert. Si acepta de forma definitiva un certificado utilizando un cliente de Rational Team Concert, AppScan Source lo reutilizará (no se le solicitará en AppScan Source que acepte un certificado). De manera similar, si acepta de forma definitiva un certificado en AppScan Source, los clientes de Rational Team Concert lo reutilizarán.

---

## **Integración de Microsoft Team Foundation Server y AppScan Source for Analysis**

La integración de Team Foundation Server con AppScan Source for Analysis precisa de una instalación de cliente de Microsoft Visual Studio Team Explorer en el sistema local.

Para configurar una conexión con Team Foundation Server, vaya al separador Team Foundation Server de las preferencias del sistema de seguimiento de defectos; también puede enviar un defecto y se le solicitará que inicie una sesión y que configure la conexión.

Las preferencias de Team Foundation Server también le permiten configurar valores de campos preestablecidos que se utilizarán durante el envío de defectos. Esto le permite establecer los valores que desea utilizar para cada defecto y modificar los valores predeterminados que se suministran con AppScan Source.

### **Envío de defectos a Microsoft Team Foundation Server**

Puede enviar paquetes con uno o varios resultados a Team Foundation Server y también puede enviar resultados individuales. La primera vez que envíe un resultado de AppScan Source for Analysis a Team Foundation Server, deberá iniciar una sesión con su nombre de usuario y contraseña. Si desea configurar los valores de campos preestablecidos que se utilizarán durante el envío, puede hacerlo en las preferencias de Team Foundation Server.

#### **Acerca de esta tarea**

Cuando envía un paquete a Team Foundation Server, el número del elemento de trabajo se asocia a los resultados específicos del paquete, no al paquete propiamente dicho. Esto garantiza que pueda seguir manipulando el paquete mientras se conserva la asociación de resultados específicos a números de elementos de trabajo.

**Nota:** Al configurar el inicio de sesión para Team Foundation Server 2010, el URL del servidor debe contener la Recopilación de proyecto de equipo a la que se desea conectar. Por ejemplo, `http://myserver:8080/tfs/Recopilación_predeterminada`.

#### **Procedimiento**

1. Seleccione uno o varios resultados de la tabla o abra el paquete. (Si abre el paquete, seleccione los resultados del paquete que desea enviar.)

2. Pulse con el botón derecho en la selección y elija **Enviar defecto > Asignar a Team Foundation Server** en el menú.
3. El cuadro de diálogo de envío le guiará por el proceso, incluido el inicio de sesión, si es necesario, y la especificación de los campos necesarios.

## Resultados

Se añadirá automáticamente un paquete al elemento de trabajo enviado, que podrá abrir posteriormente un usuario de AppScan Source for Analysis o AppScan Source for Development

---

## Cómo trabajar con defectos enviados

Cuando envía varios resultados como defectos separados, el proceso se ejecuta como proceso de fondo mientras continúa el proceso de selección. Tras el envío de los defectos, se adjunta un ID de defecto recibido del sistema de defectos a los resultados relevantes, y dicho ID permanece junto a cada resultado. Para trabajar con un defecto enviado al sistema de seguimiento de defectos, siga los pasos de este tema.

### Procedimiento

1. Abra el sistema de seguimiento de defectos y localice el defecto.
2. Guarde el archivo adjunto como un archivo de paquete AppScan Source (.ozbd1). Puede abrir este archivo en AppScan Source for Analysis o como un paquete en AppScan Source for Development.

---

## Envío de paquetes para el seguimiento de defectos y por correo electrónico

Los resultados de los paquetes se pueden enviar al sistema de seguimiento de defectos de la empresa o se pueden enviar por correo electrónico. Cuando haya colocado los resultados en un paquete, puede enviar estos resultados como errores para su remediación por parte del desarrollador.

### Procedimiento

1. Abra el paquete.
2. Pulse la flecha hacia abajo del botón de la barra de herramientas **Enviar paquete al rastreo de defecto** y, a continuación, seleccione su sistema de seguimiento de defectos.

**Nota:** En función de su sistema de seguimiento de defectos, es posible que desee modificar las preferencias del sistema de seguimiento de defectos antes de enviar el paquete.

Como alternativa, en la barra de herramientas de Paquete, pulse **Enviar paquete por correo electrónico** para enviar el paquete a otros usuarios (se deben configurar previamente las preferencias de correo electrónico).

3. Complete los recuadros de diálogo de configuración que se vayan abriendo. Estos varían en función del sistema de seguimiento de defectos que haya elegido, y se describen en la sección *AppScan Source for Analysis y seguimiento de defectos* de la ayuda.

---

## Seguimiento de defectos a través de correo electrónico (enviando los resultados por correo electrónico)

### Acerca de esta tarea

Si ha configurado las preferencias del correo electrónico, puede enviar resultados o paquetes por correo electrónico directamente a los desarrolladores para avisarles de defectos potenciales encontrados tras un escaneo. El correo electrónico incluye un archivo adjunto que contiene los resultados y texto que describe dichos resultados.

**Nota:** Algunos sistemas SMTP (Simple Mail Transfer Protocol) solo envían correo a dominios específicos. En este caso, si realiza el envío desde `mydomain.com`, solo los destinatarios de `mydomain.com` pueden recibir el correo electrónico a través de AppScan Source for Analysis.

Para enviar por correo electrónico los resultados de una tabla de resultados :

### Procedimiento

1. Seleccione uno o varios resultados de la tabla o abra un paquete. Si abre un paquete, seleccione los resultados del paquete que desea enviar por correo electrónico.
2. Pulse con el botón derecho en la selección y elija **Enviar resultados por correo electrónico** en el menú.
3. El correo electrónico incluirá un archivo adjunto que contiene los resultados. En el cuadro de diálogo Nombre del archivo adjunto, especifique un nombre para el paquete de resultados. Por ejemplo, especificar `mi_resultado` en el campo **Nombre del archivo adjunto** hace que se adjunte al correo electrónico un paquete con el nombre de archivo `mi_resultado.ozbdl`. Pulse **Aceptar** para abrir el cuadro de diálogo Enviar resultados por correo electrónico.
4. De forma predeterminada, el campo **Enviar a** del cuadro de diálogo Enviar resultados por correo electrónico se llenará con la **A dirección** que se especifica en las preferencias de correo electrónico. Sin embargo, se puede cambiar fácilmente al preparar el correo electrónico. En este cuadro de diálogo, revise el contenido del correo electrónico y pulse en **Aceptar** para enviar el correo electrónico.

### Resultados

Contenido de un correo electrónico de ejemplo:

```
1 findings:
Name: JavaAny.test_DataInput
Type: Vulnerability.Validation.Required
Severity: Low
Classification: Suspect
File Name: C:\TestApps\java\JavaAny\src\JavaAny.java
Line / Col: 275 / 0
Context: di . java.io.DataInput.readFully ( ba )
Notes: Check into this vulnerability and report back ASAP.
```

**Consejo:** Puede enviar resultados individuales o paquetes por correo electrónico desde la vista Detalle de resultado. También puede enviar por correo electrónico paquetes pulsando **Enviar paquete por correo electrónico** en la barra de herramientas del Paquete.

---

## Capítulo 8. Informes de resultados e informes de auditoría

Los analistas de seguridad y los gestores de riesgos pueden acceder a informes de resultados seleccionados o a una serie de informes de auditoría que calibran la conformidad con las prácticas recomendadas sobre seguridad de software y los requisitos reguladores. En esta sección se explica cómo crear informes de datos de resultados agregados.

AppScan Source for Analysis genera dos tipos de informes: los informes de resultados y los informes de AppScan Source. Un *informe de resultados* es un informe de resultados seleccionados. Un *Informe de AppScan Source* es un informe basado en las agrupaciones por categorías de todos los resultados adaptados a una política de seguridad específica. Los informes de AppScan Source se listan en “Informes de AppScan Source” en la página 225.

Los informes ofrecen los detalles sobre resultados obtenidos durante un determinado escaneo y todos los informes de AppScan Source pueden contener notas y datos de rastreo añadidos a los resultados. La longitud del informe depende del número de resultados incluidos en el mismo. Puede generar informes como archivos PDF o en Hypertext Markup Language (HTML). Los informes HTML funcionan como páginas web en las que puede saltar a una sección pulsando un botón o un enlace. Luego puede navegar por la información utilizando las funciones de navegación que ofrecen los navegadores web.

Los informes también listan los filtros de escaneo-tiempo que se han aplicado a los resultados. Los filtros de escaneo-tiempo se describen en “Determinación de filtros aplicados” en la página 168.

---

### Crear informes de resultados

#### Acerca de esta tarea

Después de realizar un escaneo, es posible que desee generar informes sobre las vulnerabilidades identificadas. Puede generar varios informes de resultados:

- Findings
- Findings by Type
- Findings by Classification
- Findings by File
- Findings by API
- Findings by Bundle
- Resultados por CWE (Common Weakness Enumeration)
- DTS Activity

**Nota:** Los informes de resultados muestran resultados detallados por categoría, de forma parecida a los resultados de la tabla de resultados. La generación de los informes de resultados es una operación con gran actividad de memoria (relacionada con <https://xmlgraphics.apache.org/fop/1.1/running.html#memory>) que podría precisar de hasta 1024 MB de memoria adicional del sistema. Si está generando un informe para un escaneo de una aplicación de gran tamaño y se da cuenta de que hay problemas de memoria, puede escanear partes de la aplicación

por separado o alterar la configuración de escaneo y, a continuación, puede intentar generar el informe o informes de nuevo.

Los hipervínculos de ID de CWE del informe de resultados conectan con el sitio web de CWE en <http://cwe.mitre.org/>.

Para generar un informe de resultados:

## Procedimiento

1. En una vista que contenga resultados, seleccione los resultados que desea incluir en el informe. Si no selecciona ningún resultado, el informe contendrá todos los resultados de la vista activa.

En el menú **Herramientas**, pulse **Generar informe de resultados**. Como alternativa, en vistas que contengan resultados, seleccione y pulse con el botón derecho en un conjunto de resultados y luego seleccione **Generar informe de resultados** en el menú.

2. En el cuadro de diálogo **Seleccionar informe de resultados**, seleccione un tipo de informe.

Pulse **Finalizar** para generar el informe, o pulse **Siguiente** para especificar estos valores opcionales en la página Especificar destino y Hoja de estilo:

- Puede especificar el destino y el formato del informe. Puede generar el informe en formato HTML, como un archivo ZIP que contiene todos los componentes del informe HTML o un PDF (debe tener Adobe Acrobat Reader para poder ver informes PDF). Si no especifica un destino y el formato del informe (o pulsa **Finalizar** en la página Seleccionar informe de resultados), se selecciona HTML de forma predeterminada, y el informe se guarda en `<data_dir>\reports` (donde `<data_dir>` es la ubicación de los datos de programa AppScan Source, como se describe en “Instalación y ubicaciones de archivo de datos de usuario” en la página 335).

**Nota:** Si está creando un informe personalizado (en lugar de un informe de resultados) en formato PDF, puede especificar el nivel de detalle que se ha de incluir en el informe:

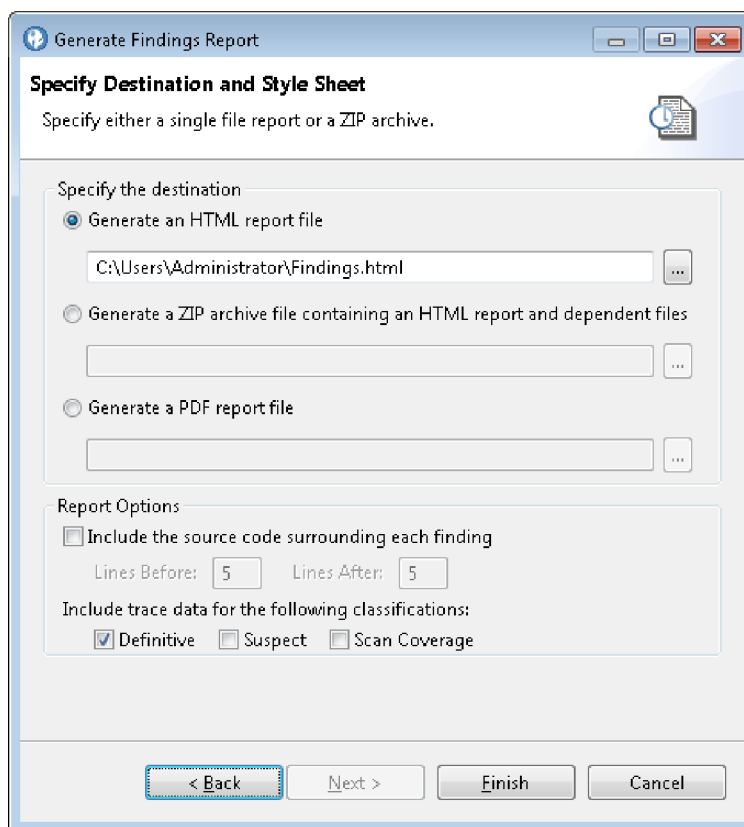
- **Resumen:** contiene recuentos para cada grupo del informe
- **Detallado:** contiene recuentos para cada API para cada propiedad de vulnerabilidad
- **Completo:** contiene tablas que constan de cada resultado para cada API
- **Anotado:** contiene todos los resultados y las notas, datos de rastreo o fragmentos de código incluidos con los resultados
- Para incluir un fragmento de código en el informe, seleccione **Incluir el código fuente de cada resultado** e indique el número de líneas por encima y por debajo de la línea de código vulnerable que hay que añadir en el informe.

**Consejo:** En la sección Informes de la vista Detalle del resultado también puede definir el número de líneas de código que se deben incluir en el informe después de los resultados.

Después de generar el informe, cuando amplía un resultado que contiene notas o fragmentos de código, el código fuente aparece bajo el resultado en un recuadro azul o bajo la nota amarilla. El texto rojo en negrita resalta la línea de código vulnerable.



- Para incluir datos de rastreo de AppScan Source en el informe, seleccione una o más de las clasificaciones (**Definitivo**, **Sospechoso** o **Cobertura de escaneo**) en **Incluir datos de rastreo para las clasificaciones siguientes**. Pulse **Finalizar** para generar el informe.



## Informes de AppScan Source

Los informes de AppScan Source ayudan a los analistas de seguridad de software, gestores de despliegue y auditores de gestión de riesgos a medir la conformidad con las prácticas recomendadas sobre seguridad de software y los requisitos reguladores. Los informes de AppScan Source ayudan a garantizar que las aplicaciones críticas cumplen con los estándares de seguridad establecidos.

AppScan Source utiliza los resultados del análisis de vulnerabilidad del código fuente para potenciar una serie de informes que ofrecen una imagen detallada de la conformidad al profesional de seguridad, despliegue o auditoría.

Los informes de AppScan Source ofrecen:

- Tarjeta de informe: tarjeta de informe para una vista abreviada del estado de seguridad de cada categoría principal
- Revisión de auditoría detallada: una auditoría detallada de los resultados no conformes
- Profundización: acceso directo al código no conforme para analizarlo con mayor profundidad y establecer prioridades de remediación y asignación

AppScan Source for Analysis genera diferentes informes de AppScan Source:

- “Informe de CWE/SANS Top 25 2011” en la página 227

- “Informe DISA Application Security and Development STIG V3R10” en la página 228
- “Informe Web Application Security Project (OWASP) Mobile Top 10” en la página 228
- “Informe Web Application Security Project (OWASP) Top 10 2013” en la página 228
- “Informe de Payment Card Industry Data Security Standard (PCI DSS) Versión 3.2” en la página 228
- “Informe de Software Security Profile” en la página 228: ofrece una visión general del estado de seguridad de una aplicación entre las principales categorías de vulnerabilidad.

## Creación de un informe personalizado de AppScan Source

### Procedimiento

1. En el menú **Herramientas**, pulse **Generar informe**.
2. En el cuadro de diálogo Generar informe, seleccione un informe de AppScan Source:

- **CWE SANS Top 25 2011**
- **DISA Application Security and Development STIG V3R10**
- **OWASP Mobile Top 10**
- **OWASP Top 10 2013**
- **PCI Data Security Standard V3.2**
- **Software Security Profile**

Pulse **Finalizar** para generar el informe, o pulse **Siguiente** para especificar estos valores opcionales en la página Especificar destino y Hoja de estilo:

- Puede especificar el destino y el formato del informe. Puede generar el informe en formato HTML, como un archivo ZIP que contiene todos los componentes del informe HTML o un PDF (debe tener Adobe Acrobat Reader para poder ver informes PDF). Si no especifica un destino y el formato del informe (o pulsa **Finalizar** en la página Seleccionar informe de resultados), se selecciona HTML de forma predeterminada, y el informe se guarda en <data\_dir>\reports (donde <data\_dir> es la ubicación de los datos de programa AppScan Source, como se describe en “Instalación y ubicaciones de archivo de datos de usuario” en la página 335).

**Nota:** Si está creando un informe personalizado (en lugar de un informe de resultados) en formato PDF, puede especificar el nivel de detalle que se ha de incluir en el informe:

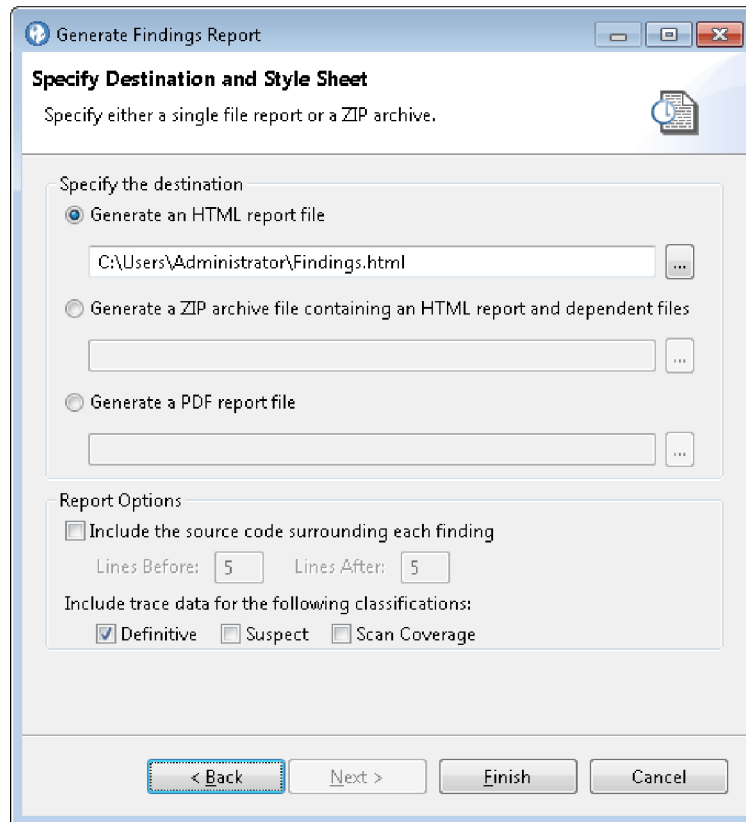
- **Resumen:** contiene recuentos para cada grupo del informe
- **Detallado:** contiene recuentos para cada API para cada propiedad de vulnerabilidad
- **Completo:** contiene tablas que constan de cada resultado para cada API
- **Anotado:** contiene todos los resultados y las notas, datos de rastreo o fragmentos de código incluidos con los resultados
- Para incluir un fragmento de código en el informe, seleccione **Incluir el código fuente de cada resultado** e indique el número de líneas por encima y por debajo de la línea de código vulnerable que hay que añadir en el informe.

**Consejo:** En la sección Informes de la vista Detalle del resultado también puede definir el número de líneas de código que se deben incluir en el informe después de los resultados.

Después de generar el informe, cuando amplía un resultado que contiene notas o fragmentos de código, el código fuente aparece bajo el resultado en un recuadro azul o bajo la nota amarilla. El texto rojo en negrita resalta la línea de código vulnerable.

- Para incluir datos de rastreo de AppScan Source en el informe, seleccione una o más de las clasificaciones (**Definitivo**, **Sospechoso** o **Cobertura de escaneo**) en **Incluir datos de rastreo para las clasificaciones siguientes**.

Pulse **Finalizar** para generar el informe.



## Informe de CWE/SANS Top 25 2011

El informe CWE/SANS Top 25 2011 se basa en los *25 errores de software más peligrosos de CWE/SANS 2011*.

Para obtener más información sobre los *25 errores de software más peligrosos de CWE/SANS 2011*, consulte <http://cwe.mitre.org/top25/>.

Para saber más sobre todas las debilidades CWE (Common Weakness Enumeration) a las que AppScan Source da soporte, consulte Capítulo 15, “Soporte a CWE”, en la página 339.

## **Informe DISA Application Security and Development STIG V3R10**

Este tema proporciona enlaces a documentos de ayuda y sitio web de Defense Information Systems Agency (DISA) Application Security y Development Security Technical Implementation Guide (STIG).

Para obtener más información sobre DISA Application Security and Development STIG, consulte <http://iase.disa.mil/>.

## **Informe Web Application Security Project (OWASP) Top 10 2013**

Este tema proporciona enlaces a documentos de ayuda y sitio web de Open Web Application Security Project (OWASP).

Para obtener más información acerca de OWASP, consulte [https://www.owasp.org/index.php/Main\\_Page](https://www.owasp.org/index.php/Main_Page). Los enlaces a varios documentos OWASP y de riesgos de seguridad están disponibles en [https://www.owasp.org/index.php/Category:OWASP\\_Top\\_Ten\\_Project](https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project).

## **Informe Web Application Security Project (OWASP) Mobile Top 10**

Este tema proporciona enlaces a documentos de ayuda y sitio web de Open Web Application Security Project (OWASP).

Para obtener más información sobre OWASP Mobile Security Project, consulte [https://www.owasp.org/index.php/OWASP\\_Mobile\\_Security\\_Project](https://www.owasp.org/index.php/OWASP_Mobile_Security_Project).

## **Informe de Payment Card Industry Data Security Standard (PCI DSS) Versión 3.2**

Este informe proporciona datos relevantes necesarios para garantizar la conformidad con Payment Card Industry Data Security Standard (PCI DSS).

Consulte el apartado [https://www.pcisecuritystandards.org/security\\_standards/index.php](https://www.pcisecuritystandards.org/security_standards/index.php) para obtener más información.

## **Informe de Software Security Profile**

Software Security Profile presenta un completo análisis de las características de la aplicación que resultan especialmente relevantes para su seguridad. Proporciona una auditoría detallada de las características de seguridad críticas del software para un determinado proyecto. Este informe le ayuda a verificar la implementación de requisitos como cifrado, control de acceso, inicio de sesión y manejo de errores antes de certificar el software para su despliegue.

El compuesto identifica zonas de riesgo potencial y presenta recomendaciones para minimizar los riesgos. El informe permite facilitar un asesoramiento de la seguridad global de la aplicación que resulta útil para las revisiones de conformidad, política y arquitectura. Los resultados se basan en un completo análisis estático del código fuente, utilizando una base de datos de fallos, vulnerabilidades, estándares específicos de la industria y prácticas recomendadas generales.

Software Security Profile muestra la siguiente información:

- Tarjeta de informe: contiene enlaces con los detalles del informe e indicadores de gravedad que resumen la sección.
- Visión general: resume el objetivo del informe y describe la configuración de la aplicación.
- Métricas: identifica el número total de paquetes, clases, métodos y líneas de código de todos los paquetes del proyecto.
- Resultados detallados por categoría: muestra cada categoría de vulnerabilidad encontrada dentro de un nombre de categoría de vulnerabilidad y un icono que indica el nivel de gravedad de la vulnerabilidad.



---

## Capítulo 9. Creación de informes personalizados

En el Editor de informe, puede crear plantillas de informe utilizadas para crear informes personalizados.

Es posible que un informe de resultados de AppScan Source o un informe de AppScan Source no proporcione los datos exactos que necesita; puede necesitar que el informe contenga más o menos información. El Editor de informes de AppScan Source for Analysis permite crear informes personalizados.

Generalmente, se crea un informe personalizado cuando se necesita:

- Generar un informe que se correlacione y notifique una política de seguridad exclusiva. Primero debe crear un informe personalizado y luego aplicar el informe a un asesoramiento específico.
- Definir y producir un informe para resaltar resultados y características únicos.
- Modificar o añadir un informe existente.

Cuando guarda la plantilla del informe en `<data_dir>\reports` (donde `<data_dir>` es la ubicación de los datos de programa AppScan Source, como se describe en “Instalación y ubicaciones de archivo de datos de usuario” en la página 335), el informe está disponible para asesoramientos de cualquier aplicación. Cuando se guarda en un directorio de una determinada aplicación, el informe está disponible para escaneos de dicha aplicación o de cualquiera de sus proyectos.

Antes de empezar a crear o editar un informe de AppScan Source, familiarícese con los tipos de informe y con los elementos que comprenden cada informe. Cuando crea un informe personalizado, puede correlacionar elementos del informe en cualquier orden. Los elementos del informe incluyen información sobre resultados, fragmentos de código, rastreo y contenido de remediación, así como texto y elementos gráficos.

---

### Editor de informe

Con el Editor de informes, puede editar informes o plantillas personalizados o crear un nuevo informe. Los informes personalizados incluyen elementos que están disponibles en un informe de resultados, tales como la información de los resultados, los fragmentos de códigos, el contenido de remediación y rastreo de AppScan Source, al igual que una matriz de vulnerabilidad. Antes de empezar a diseñar nuevos informes, se recomienda familiarizarse con el proceso de creación de informes, modificando una plantilla de informe existente en el Editor de informes.

El Editor de informe consta de los separadores Diseño de informe, Categorías y Vista previa.

- **Diseño de informe:** diseñar el aspecto del informe. En el diseño puede añadir, eliminar o reordenar elementos del informe de AppScan Source.
- **Categorías:** crear y editar categorías. Una *categoría* es un grupo de resultados. La categoría identifica los resultados que se deben incluir en el informe, cómo agrupar dichos resultados y el orden de agrupación.
- **Vista previa:** mirar el informe correspondiente al asesoramiento actual mientras se edita.

Los tres separadores contienen campos comunes:

- **Archivo:** vía de acceso del archivo de agrupación guardado (solo lectura). No se muestra nada en este campo hasta que se ha guardado el archivo. Una vez guardado, el archivo de agrupación es un archivo XML que define el informe.
- **Nombre:** nombre del informe definido por el usuario.

Los botones de la barra de herramientas para guardar, abrir, crear, copiar y generar informes personalizados incluyen:

- **Crear un nuevo informe:** crea un nuevo informe personalizado
- **Nuevo informe a partir de uno existente:** crea un nuevo informe personalizado a partir de una plantilla de informe existente
- **Abrir un informe guardado:** abre un archivo de agrupación para editarlo
- **Guardar:** guarda el informe actual en el archivo especificado
- **Guardar como:** guarda el informe actual en un archivo nuevo
- **Generar una instancia de este informe:** crea una copia del informe para el asesoramiento actualmente abierto

**Consejo:** Para ver ejemplos de informes existentes, pulse **Nuevo informe a partir de uno existente** y, a continuación, elija una de las plantillas de informes de AppScan Source. Si explora los separadores Diseño de informe y Categorías en las plantillas puede ver cómo están diseñados los informes.

## Separador Diseño de informe

El separador Diseño de informe consta de las secciones Paleta y de secciones que le permiten especificar una cabecera o pie de página que aparecerá en cada página.

### Cabecera de página y Pie de página

El campo **Cabecera de página** le permite especificar el texto que aparece en la parte superior de cada página de un informe y el campo **Pie de página** le permite especificar el texto que aparece en la parte inferior de cada página.

### Paleta

La Paleta muestra una lista de elementos que comprenden los informes estándares de AppScan Source. Algunos de los elementos sólo muestran información para las categorías que se han definido en el separador Categorías (consulte la sección Tabla 19 en la página 233).

*Tabla 18. Paleta de diseño de informe: los elementos que no dependen de las categorías*

| Elemento del informe       | Descripción                                                                                                                                     |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Cabecera de texto          | Añade un bloque de texto en negrita al diseño de informe.                                                                                       |
| Cabecera de imagen         | Muestra una imagen escalada a un tamaño especificado en píxeles.                                                                                |
| Cabecera de AppScan Source | Cabecera de informe que contiene información de marca de AppScan Source.                                                                        |
| Título y fecha             | Título de informe que incluye el nombre del elemento que se ha escaneado, junto con la fecha de escaneo y la fecha en que se generó el informe. |



Tabla 18. Paleta de diseño de informe: los elementos que no dependen de las categorías (continuación)

| Elemento del informe     | Descripción                                                                                                                         |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Bloque de texto          | Cualquier texto definido por el usuario. Una cabecera también se puede añadir para el bloque de texto en el campo <b>Etiqueta</b> . |
| Matriz de vulnerabilidad | Matriz de vulnerabilidad del asesoramiento (muestra el mismo gráfico que aparece en la vista Matriz de vulnerabilidad).             |
| Métricas                 | Identifica el número total de paquetes, clases, métodos y líneas de código de todos los paquetes del proyecto.                      |
| Historial de escaneo     | Métricas para el escaneo actual y métricas históricas para escaneos del mismo destino.                                              |

Tabla 19. Paleta de diseño de informe: elementos que dependen de categorías

| Elemento del informe       | Descripción                                                                                                                                                                                      |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tarjeta de informe         | Breve desglose de niveles de vulnerabilidad de cada categoría definida en el separador Categorías. Contiene enlaces a los detalles del informe e indicadores de gravedad que resumen la sección. |
| Desglose de vulnerabilidad | Tabla con un desglose del número de vulnerabilidades en todas las categorías definidas en el separador Categorías, por gravedad y clasificación.                                                 |
| Tarjeta de informe parcial | Desglose de niveles de vulnerabilidad de categorías especificadas por el usuario como se ha especificado en el separador Categorías.                                                             |
| Categorías                 | Lista todos los datos de resultados categorizados, tal como se han especificado en el separador Categorías.                                                                                      |
| Categoría                  | Lista todos los resultados en una o más categorías que se han definido en el separador Categorías.                                                                                               |

## Diseño

A medida que añade elementos de la paleta, aparecen en el diseño. Utilice la barra de herramientas de la sección para eliminar, modificar o mover elementos en el diseño.

## Separador Categorías

Mediante el separador Categorías, puede añadir categorías que contienen resultados basados en paquetes, propiedades, o los resultados seleccionados que seleccione. A continuación, se pueden utilizar las categorías cuando se añaden determinados elementos al diseño. Por ejemplo, cuando añade un Desglose de vulnerabilidad al diseño, se añade al diseño una tabla con un desglose del número de vulnerabilidades en todas las categorías (por gravedad y clasificación). El separador Categorías consta de un panel con un árbol de categorías y un panel en

el que se pueden editar los atributos de la categoría seleccionada. Cada categoría contiene los resultados del asesoramiento que satisfacen ciertos requisitos definidos por el usuario.

Las categorías disponibles incluyen:

- **Paquete:** la categoría de paquete consta de una lista de nombres de paquete. Cualquier resultado de un paquete cuyo nombre aparece en la lista aparece en esta categoría. Aunque se eligen paquetes procedentes del asesoramiento actual, puede aplicar la categoría de paquete a cualquier asesoramiento, puesto que los paquetes se comparan por nombre.
- **Resultados individuales:** elija los resultados específicos que desea añadir a la categoría. Al informe solo se añade una instantánea del resultado. Si modifica el resultado después de añadirlo al informe, este no refleja el campo.
- **Propiedades Tipos de vulnerabilidad, Mecanismos y Tecnologías:** seleccione conjuntos de propiedades y propiedades necesarias de las API de la Base de datos de conocimientos de AppScan Source Security. Si un resultado contiene al menos una de las **Propiedades** y todas las **Propiedades necesarias**, se incluye en el informe.

Esta tabla identifica los paneles de categorías y los elementos de que consta el panel.

*Tabla 20. Atributos del separador Categorías*

| Atributo                                   | Descripción                                                                                                                                                                                                                    | Cómo editarlo                                                                                                                                                                                     |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Etiqueta                                   | El nombre abreviado de la categoría, por ejemplo, Desbordamiento de almacenamiento intermedio. La etiqueta identifica la categoría en la lista de árbol de categorías y es la cabecera de categoría del informe personalizado. | Escriba una etiqueta en un campo de texto de una sola línea.                                                                                                                                      |
| Resumen                                    | Una plantilla para una frase que indique cuántos resultados se notifican en esta categoría. El recuento real sustituye %FindingCount% durante la generación del informe.                                                       | Escriba una breve descripción de la categoría y pulse <b>Añadir cuenta</b> para colocar la variable %FindingCount% en la frase en la posición del cursor.                                         |
| Texto                                      | Breve descripción de la categoría.                                                                                                                                                                                             | Especifique el texto que describe la categoría.                                                                                                                                                   |
| Propiedades (solo categorías de propiedad) | Los resultados que tengan al menos una de estas propiedades se notificarán en esta categoría. Si un resultado no tiene todas las propiedades necesarias listadas, el resultado no se incluye en esta categoría.                | Pulse <b>Añadir</b> en la barra de herramientas y seleccione una propiedad del cuadro de diálogo Añadir propiedades. Pulse <b>Eliminar</b> para eliminar de la lista los elementos seleccionados. |

Tabla 20. Atributos del separador Categorías (continuación)

| Atributo                                              | Descripción                                                                                                                     | Cómo editarlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Propiedades necesarias (solo categorías de propiedad) | Los resultados que tienen todas las propiedades necesarias y al menos una propiedad aparecen en el informe bajo esta categoría. | Pulse <b>Añadir</b> en la barra de herramientas y seleccione una propiedad del cuadro de diálogo Añadir propiedades. Pulse <b>Eliminar</b> para eliminar de la lista los elementos seleccionados.                                                                                                                                                                                                                                                                                                                                                                                                  |
| Paquetes (solo categorías de paquete)                 | Especifica los nombres de los paquetes que se deben incluir en esta categoría.                                                  | Pulse <b>Añadir un paquete</b> en la sección Paquetes y seleccione los paquetes en la lista.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Resultados (solo de categorías de resultados)         | Especifica los resultados que se deben incluir en esta categoría.                                                               | <p>Seleccione los resultados de cualquier tabla de resultados y, a continuación, pulse <b>Añadir resultados</b> en la barra de herramientas de la tabla para añadir los resultados seleccionados. Si más de una vista contiene los resultados seleccionados, se le solicitará que seleccione la vista que contiene los resultados seleccionados que desea añadir.</p> <p>También puede arrastrar los resultados de una tabla de resultados a la tabla de la vista Editor de informes, en el Editor de informes o directamente a una categoría de resultados existente del árbol de categorías.</p> |

## Separador Vista previa

Puede realizar una vista previa de los informes de AppScan Source for Analysis a medida que edita sus plantillas. En el panel Vista previa, pulse **Vista previa** para ver el informe correspondiente a un asesoramiento abierto.

## Generación de informes personalizados

Los procedimientos de temas de esta sección describen cómo diseñar y generar un informe a partir de un informe personalizado existente. Como alternativa, puede crear un informe nuevo. Para editar un informe existente, abra el informe y siga los procedimientos de diseño, modificación y vista previa.

- “Diseño de un informe a partir de un informe personalizado existente” en la página 236
- “Inclusión de categorías en el informe” en la página 236
  - “Adición de paquetes a una categoría” en la página 236
  - “Adición de resultados a una categoría” en la página 237
  - “Adición de propiedades a una categoría” en la página 237
- “Vista previa del informe” en la página 237

- “Cómo guardar la plantilla del informe” en la página 237

## Diseño de un informe a partir de un informe personalizado existente

### Procedimiento

1. En la vista Editor de informe, pulse **Nuevo informe a partir de uno existente** en la barra de herramientas.
2. Seleccione una plantilla de informe en la lista de informes existentes. En el panel Diseño, realice una vista previa de la plantilla del informe.
3. Cambie el nombre del informe, las cabeceras y pies de página o elementos de la plantilla:
  - a. Añada una **Cabecera de página** o **Pie de página**. Las cabeceras y los pies de página aparecen en cada página.
  - b. Añada elementos adicionales al informe. Seleccione los elementos del informe que desee en la **Paleta** y pulse **Insertar** (cada elemento debe insertarse por separado).
  - c. Suprima elementos del informe. Seleccione los elementos que desea eliminar de la plantilla y pulse el botón de la barra de herramientas **Eliminar el elemento del informe seleccionado**.
4. Reordene los elementos del informe. Seleccione un elemento en la vista previa y pulse **Subir el elemento de informe seleccionado** o **Bajar el elemento de informe seleccionado** en la barra de herramientas para subir o bajar el elemento de informe.
5. Realice una doble pulsación en un elemento en el panel Diseño para editarlo o seleccione el elemento y luego pulse **Editar el elemento del informe seleccionado** en la barra de herramientas.

En el cuadro de diálogo resultante, realice los cambios que desee. Por ejemplo, para editar un bloque de texto, realice cambios en el cuadro de diálogo Editar bloque de texto modificando la etiqueta y el texto descriptivo.

**Nota:** Algunos elementos no se pueden modificar.

## Inclusión de categorías en el informe

Cuando haya definido el diseño, determine las categorías que desea incluir en el informe.

### Procedimiento

1. En el panel Categorías, pulse **Crear una nueva categoría de propiedades**, **Crear una nueva categoría de paquetes** o **Crear una nueva categoría de resultados**.
2. Asigne un nombre a la categoría escribiendo una etiqueta para la categoría, un breve resumen de la categoría que contenga un recuento y texto descriptivo.  
Suba o baje una categoría o subcategoría utilizando los botones de flecha de la barra de herramientas.
3. Añada los paquetes, resultados o propiedades a la categoría.

### Adición de paquetes a una categoría

#### Procedimiento

1. Abra un asesoramiento que contenga paquetes. Si el asesoramiento aún no contiene ningún paquete, no puede añadir un paquete al informe.

2. En el panel Paquetes, pulse **Añadir un paquete** y especifique los paquetes que desea incluir en esta categoría.

## Adición de resultados a una categoría

### Procedimiento

1. Abra la vista de resultados que contiene los resultados que desea añadir. Seleccione los resultados que desee y arrástrelos a la tabla de resultados o al nodo del árbol de categorías del Editor de informes.
2. Como alternativa, pulse **Añadir resultados** en la barra de herramientas sobre la tabla de resultados para incluir los resultados seleccionados en otras vistas. Si ha seleccionado resultados en varias vistas, debe seleccionar la vista que contiene los resultados añadidos a la categoría.
3. Seleccione los resultados de cualquier vista que contenga una tabla de resultados.

## Adición de propiedades a una categoría

### Procedimiento

1. Pulse **Añadir una propiedad** (las propiedades incluyen las Vulnerabilidades, los Mecanismos y las Tecnologías). Cuando selecciona una propiedad, aparece la descripción de la base de datos de conocimientos de dicha propiedad, si está disponible.
2. Elija un mínimo de una propiedad y las propiedades necesarias. Un resultado debe tener todas las propiedades de la lista **Propiedades necesarias** para que se incluya en la categoría.

Para crear una subcategoría, seleccione una categoría y pulse los botones de flecha izquierda o derecha de la barra de herramientas.

## Vista previa del informe

Cuando diseña un informe personalizado, puede realizar una vista previa del mismo antes de generar el informe final. En el panel Vista previa, pulse **Vista previa** para ver el informe correspondiente al asesoramiento actualmente abierto.

## Cómo guardar la plantilla del informe

En la barra de herramientas de la vista Editor de informes, puede pulsar **Guardar** para conservar la plantilla del informe actual o **Guardar como** para guardar la plantilla del informe actual en un nuevo archivo.

Si guarda la plantilla del informe en el mismo directorio que un archivo de aplicación (.paf o .gaf), estará disponible en la lista de opciones del asistente de informe personalizado y en la vista Editor de informes y se podrá utilizar en siguientes escaneos de dicha aplicación. Si la guarda en <data\_dir>\reports (donde <data\_dir> es la ubicación de los datos de programa AppScan Source, como se describe en “Instalación y ubicaciones de archivo de datos de usuario” en la página 335), estará disponible para escaneos de cualquier aplicación.



---

## Capítulo 10. Personalización de la base de datos de vulnerabilidad y de las reglas de patrón

En esta sección se describe cómo personalizar la base de datos y cómo integrar vulnerabilidades personalizadas y otras rutinas en escaneos.

El proceso de escaneo incluye varias fases:

- Se ejecuta un escaneo específico del lenguaje utilizando la base de datos de vulnerabilidad (o la Base de datos de conocimientos de AppScan Source Security).
- Se ejecuta un rastreo utilizando la base de datos de vulnerabilidad.
- Se ejecuta un escaneo basado en patrones utilizando reglas de patrón de la biblioteca de reglas de patrón globales.

Puede utilizar reglas personalizadas para adaptar la Base de datos de conocimientos de AppScan Source Security a sus estándares de seguridad específicos y aplicar dichos estándares de forma coherente en toda la empresa. También puede personalizar reglas de patrón.

---

### Ampliación de la Base de datos de conocimientos de AppScan Source Security

En esta sección se describe cómo personalizar la base de datos y cómo integrar vulnerabilidades personalizadas y otras rutinas en escaneos. Las reglas personalizadas adaptan la Base de datos de conocimientos de AppScan Source Security (o la base de datos de vulnerabilidades) a sus estándares de seguridad específicos y aplican dichos estándares de forma coherente a toda la empresa.

Suele ser importante especificar sus propias rutinas de validación y codificación o definir ciertas interfaces de programación de aplicaciones (API) como vulnerabilidades, receptores y orígenes, propagadores corruptos o elementos informativos. Cuando crea estas reglas, personaliza y amplía la base de datos de vulnerabilidades de AppScan Source, parte integral de la Base de datos de conocimientos de AppScan Source Security. Cuando añade una regla personalizada a la base de datos, AppScan Source for Analysis la identifica durante el escaneo. Las llamadas a la API personalizada se revelan como resultados de seguridad o resultados de cobertura de escaneo y, a continuación, se informa sobre dichos resultados.

Por ejemplo, un analista puede añadir una API llamada `readBuffer( )`, que constituye un tipo de `BufferOverflow`. Los siguientes escaneos harán referencia a esta nueva API cuando AppScan Source for Analysis encuentre una vulnerabilidad que se ajuste a su especificación. Para obtener más detalles sobre tipos de vulnerabilidad, consulte Base de datos de conocimientos de AppScan Source Security (seleccione **Ayuda > Base de datos de conocimiento de Security** en el menú de entorno de trabajo principal).

Cuando añade rutinas de validación y codificación personalizadas, AppScan Source for Analysis deja de tratar los datos que entran y salen de estas rutinas como vulnerables. Al añadir una rutina personalizada a la base de datos de

conocimientos, AppScan Source for Analysis determina si los datos fluyen de un origen de entrada corrupta a una salida sin validación o codificación.

**Nota:** La Base de datos de conocimientos de AppScan Source Security no proporciona ayuda en línea para los registros personalizados, pero muestra ayuda para el tipo de vulnerabilidad.

**Importante:** Debe tener permisos de gestión de base de datos de conocimientos para realizar cambios en la Base de datos de conocimientos de AppScan Source Security.

## Creación de reglas personalizadas

En la vista Reglas personalizadas, puede abrir el Asistente de reglas personalizadas, una herramienta que le guiará por el proceso de creación de registros de base de datos personalizados. Cuando haya creado reglas personalizadas, las podrá ver en la vista Reglas personalizadas. La tabla muestra la firma, el lenguaje y el objetivo.

Las rutinas de validación y codificación específicas de un proyecto solo aparecen en la vista Reglas personalizadas si el proyecto al que se aplican las reglas existe en la aplicación bajo **Todas las aplicaciones** en la vista Explorador.

- **Firma:** la firma es el nombre completo de la función. Por ejemplo, la firma de Java incluye argumentos y tipos de retorno, como por ejemplo `com.test.vulnerable.VulnClass.vulnerable(java.lang.string;int):int`.
- **Lenguaje:** C/C++, Java, Visual Basic, Classic ASP o .NET
- **Objetivo:** el tipo o tipos de registro personalizado del método dado, como por ejemplo una rutina, receptor u origen `Validation.EncodingRequired`.

**Consejo:** Si está refinando el asesoramiento de una base de código escaneando iterativamente y añadiendo reglas personalizadas y luego volviendo a escanear sin cambiar el código fuente, puede reducir significativamente el tiempo de escaneo si establece las propiedades del proyecto de modo que utilice una caché de análisis de vulnerabilidad. Para ello, marque el cuadro de selección **Habilitar memoria caché de análisis de vulnerabilidad** en las propiedades del proyecto. Para ver cómo establecer las propiedades de un proyecto, consulte las instrucciones de uso de la “Separador visión general del proyecto seleccionado” en la página 259.

## Utilización del Asistente de reglas personalizadas

El Asistente de reglas personalizadas le ayuda a añadir métodos a la Base de datos de conocimientos de AppScan Source Security. El ámbito de la mayoría de las reglas personalizadas es global (se aplica a todos los proyectos). Los resultados de no rastreo personalizados, los orígenes, los receptores y los propagadores corruptos son siempre globales. Las rutinas de validación/codificación personalizadas no son globales.

**Nota:** El Asistente de reglas personalizadas no valida las selecciones del usuario. Por ejemplo, puede definir una regla personalizada que identifique un método como propagador corrupto y receptor, lo que no constituye un caso de ejemplo válido.

El Asistente de reglas personalizadas le guía por el proceso de definir y añadir los siguientes elementos a la base de datos de conocimientos:

- Receptores y orígenes
- Propagadores corruptos



- Interfaces de programa de aplicación (API) que no son susceptibles de corrupción
- Vulnerabilidades
- API que produce resultados sin rastreo
- API que no son rutinas de validación/codificación
- Devoluciones de llamada corruptas
- Resultados informativos

## Origen (de corrupción)

Un método que proporciona entrada a un programa, que puede estar mal formada o ser maliciosa.

## Receptor (susceptible a la corrupción)

Una API que envía datos desde el programa (o desde una parte visible del programa) a un archivo, la red, una base de datos, otra biblioteca o dispositivo que puede ser susceptible de recibir entradas maliciosas.

## Propagador corrupto

El hecho de marcar un método como propagador corrupto implica que si algunos de los argumentos destinados a la API derivan de datos de entrada no validados (datos corruptos), tras la llamada los datos no constantes a los que hacen referencia los otros argumentos, así como el valor de retorno, son también potencialmente corruptos. Dichos datos se deben validar o codificar antes de que se envíen a un receptor. Esta situación suele producirse porque se copian o adjuntan datos procedentes del argumento corrupto en los otros argumentos o valores de retorno.

## No susceptible a la corrupción

El hecho de marcar una API como no susceptible a la corrupción (no un propagador corrupto) implica que una llamada a la API con un argumento derivado de datos de entrada no validados (datos corruptos) no hace que la API se comporte de forma insegura o maliciosa.

Si llegan datos corruptos a una llamada, y dicha llamada está marcada como no susceptible a la corrupción, AppScan Source pasa por alto la llamada en lo que a rastreo se refiere. El rastreo de AppScan Source no notifica un rastreo perdido y no trata los datos propagados como corruptos.

**Nota:** Se llegan datos corruptos a un método que es una rutina de no validación o codificación, un receptor, un propagador corrupto o no susceptible a la corrupción, el método se notifica como un rastreo perdido. Los argumentos no constantes y los valores de retorno pueden ser o no corruptos. El gráfico de llamadas de rastreo de AppScan Source muestra un rastreo perdido.

## Resultado sin rastreo

Método o API que siempre aparece como un resultado, pero que no produce un rastreo.

## Rutina de no validación/codificación

Si se marca una API como **Rutina de no validación/codificación**, se indica que dicha API no valida ningún dato.

## Devolución de llamada corrupta

Una devolución de llamada es una rutina del código que suele ser invocada por *otro* código (por ejemplo, desde dentro de una infraestructura de nivel inferior). La devolución de llamada se pasa como argumento al otro código y se puede invocar posteriormente, posiblemente con argumentos corruptos. Si sospecha de la posibilidad de que una devolución de llamada haya podido pasar datos corruptos a sus argumentos, puede marcarla como una devolución de llamada corrupta. Esto hace que el flujo de datos corruptos a través de la rutina resulte visible.

Una rutina marcada como devolución de llamada corrupta se analizará como si se tratara de la raíz del gráfico de llamadas (es decir, como si la hubiera llamado un llamante externo desconocido) y todos sus argumentos de entrada se considerarán corruptos. Como resultado, AppScan Source notificará resultados con rastreos que comenzarán en los argumentos a la devolución de llamada corrupta.

Si el código de la aplicación realiza una llamada a la misma rutina en otros contextos, se tratará sin consideraciones especiales en cuanto a corrupción. En otros contextos, se realizará el análisis usual.

## Informativo

Las líneas de código identificadas como resultados informativos pueden no ser vulnerables, pero se deben incluir en una auditoría de seguridad.

## Adición de una regla

En este tema se describe el procedimiento para añadir una regla personalizada utilizando el Asistente de reglas personalizadas.

## Acerca de esta tarea

**Nota:** La adición o eliminación de resultados de cobertura de escaneo o seguridad y el cambio de la gravedad afecta a la densidad V del proyecto.

## Procedimiento

1. Abra el asistente desde la vista Reglas personalizadas pulsando el botón **Iniciar el asistente de reglas personalizadas**.
2. En la página **Seleccionar aplicación, proyecto y archivo**, seleccione la **Aplicación** y el **Proyecto** a los que se aplicará la regla. Asegúrese de que la aplicación y el proyecto actuales estén relacionados con el código fuente del elemento que desea añadir a la base de datos de conocimientos. Seleccione la **Configuración** si hay alguna disponible.
3. En la sección **Ámbito**, establezca el ámbito del escaneo. En función del idioma que esté escaneando, estas son las opciones de ámbito:

Tabla 21. Opciones de archivo de proyecto por lenguaje

| Lenguaje     | Opciones de archivo de proyecto                                                                                                                                                                                                                                                                                                     |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| .NET         | <ul style="list-style-type: none"> <li>• Escanear todo el proyecto por firma de método</li> <li>• Seleccionar uno o más archivos externos al proyecto</li> </ul> <p>Un proyecto .NET incluye cualquier conjunto válido, generalmente un archivo .dll o .exe.</p>                                                                    |
| Java         | <ul style="list-style-type: none"> <li>• Escanear todo el proyecto por firma de método</li> <li>• Seleccionar uno o más archivos del proyecto</li> <li>• Seleccionar uno o más archivos externos al proyecto</li> </ul> <p>Un proyecto Java incluye archivos .jar o .class o una jerarquía de directorios de archivos de clase.</p> |
| C/C++        | <ul style="list-style-type: none"> <li>• Escanear todo el proyecto por firma de método</li> <li>• Seleccionar uno o más archivos del proyecto</li> </ul>                                                                                                                                                                            |
| Visual Basic | Escanear archivos FRM (formularios), archivos CLS (clase) y BAS (basic)                                                                                                                                                                                                                                                             |
| ASP clásico  | Escanear solo archivos ASP                                                                                                                                                                                                                                                                                                          |

- **Escanear todo el proyecto por firma de método** es la modalidad de escaneo predeterminada. Esta modalidad escanea el proyecto y devuelve todas las firmas disponibles. Esta modalidad de escaneo puede tardar bastante tiempo.
  - La opción **Seleccionar uno o más archivos del proyecto** aísla ciertos archivos de proyecto que contienen métodos que pueden necesitar reglas personalizadas.
  - La opción **Seleccionar uno o más archivos externos al proyecto** identifica archivos externos a este proyecto para incluirlos en el escaneo.
4. En la sección **Caché**, seleccione el recuadro de selección para volver a leer un proyecto modificado o un código modificado. La memoria caché de análisis de vulnerabilidad también se borrará (si el proyecto actual está establecido de modo que coloque en memoria caché el análisis de vulnerabilidad, esta se volverá a crear en el siguiente escaneo).
  5. **Análisis de la cadena**: el análisis de la cadena supervisa la manipulación de cadenas en proyectos Java o Microsoft .NET. Proporciona la detección automática de rutinas de saneamiento y validación. Con esta detección se pueden reducir los falsos positivos y negativos. Marque el cuadro de selección **Habilitar análisis de la cadena para encontrar funciones validador/saneador** para habilitar el análisis de la cadena. El cuadro de selección **Aplicar las reglas importadas al ámbito global** determina si las rutinas de saneamiento o validación descubiertas se deben aplicar a un único proyecto o a nivel general (a todos los proyectos).

**Nota:** La aplicación del análisis de cadena puede ralentizar un escaneo. Por lo tanto, se recomienda que solo se aplique tras cambios en el código y luego se inhabilite para los siguientes escaneos. Además, las rutinas descubiertas se pueden ver como *sugerencias* y los auditores las pueden revisar. Estas rutinas se pueden ver en la vista Reglas personalizadas.

6. Pulse **Siguiente** para continuar en la siguiente página del asistente.

7. En la página **Seleccionar métodos**:

- a. Seleccione el método o métodos que se añadirán a la base de datos de conocimientos. El método es el nombre de la API de vulnerabilidad.

La lista de métodos se puede filtrar de dos maneras:

- Filtrado automático: escriba el texto del filtro en el campo **Filtro**. A medida que escribas, el filtro se aplicará automáticamente a la lista de métodos. Esta es la modalidad de filtrado predeterminada.
- Filtrado manual: escriba el texto del filtro en el campo **Filtro** y, a continuación, pulse el botón **Filtro** (o pulse Intro) para aplicar el filtro a la lista. Es posible que desee utilizar el filtrado manual cuando un gran número de métodos provoque retrasos en el filtrado automático.

En ambos casos, el asterisco (\*) y la interrogación (?) se pueden utilizar como caracteres comodín. Un asterisco coincide con cualquier grupo de cero o más caracteres, mientras que una interrogación coincide con un carácter único.

Para cambiar la modalidad de filtro, utilice el botón **Filtro** como conmutador efectuando una doble pulsación o utilizando el teclado para ir hasta este y, a continuación, pulse la barra espaciadora. Cuando el filtrado manual está activado, el botón **Filtro** aparece sin pulsar y su ayuda contextual específica **Aplicar filtro (efectúe una doble pulsación o pulse espacio para filtrar automáticamente)**. Cuando el filtrado automático está activado, el botón aparece pulsado y su ayuda contextual específica **Filtrar manualmente**.

Para ver mejor la lista de métodos, las acciones de expandir y contraer están disponibles. Para expandir o contraer todo el árbol, pulse con el botón derecho del ratón sobre y seleccione **Expandir todo** o **Contraer todo**. Para expandir un paquete o clase y todas sus subentradas, pulse con el botón derecho del ratón sobre el paquete o la clase y seleccione **Expandir hijos**.

Para seleccionar varios métodos, utilice las teclas Control o Mayúsculas del teclado.

Marque el cuadro de selección **Mostrar todas las firmas** para ver la firma completa de los métodos del árbol. Por ejemplo, la firma completa de Java incluye paquete, clase, método, tipos de argumento y tipos de retorno, como por ejemplo

```
com.test.vulnerable.VulnClass.vulnerable(java.lang.string;int):int.
```

- b. Identifica si el escaneo debe marcar el método como uno de los siguientes:

- “Origen (de corrupción)” en la página 241
- “Receptor (susceptible a la corrupción)” en la página 241
- “Propagador corrupto” en la página 241
- “No susceptible a la corrupción” en la página 241
- “Resultado sin rastreo” en la página 241
- “Rutina de no validación/codificación” en la página 242
- “Devolución de llamada corrupta” en la página 242
- “Informativo” en la página 242

8. Si está añadiendo métodos como “No susceptible a la corrupción” en la página 241, “Rutina de no validación/codificación” en la página 242, “Propagador corrupto” en la página 241, o “Devolución de llamada corrupta” en la página 242, pulse **Finalizar** para añadir los registros a la Base de datos de conocimientos de AppScan Source Security.
9. Si añade métodos como por ejemplo “Origen (de corrupción)” en la página 241 o “Informativo” en la página 242:
  - a. Pulse **Siguiente** para continuar en la página **Asignar atributos de regla**.
  - b. Para cada método que haya añadido: Seleccione una o varias propiedades para asignar al método. La columna **Tipo** del método se actualizará para indicar el tipo de vulnerabilidad de los resultados que se producirán mediante la regla personalizada.

**Consejo:** Para añadir las mismas propiedades a varios métodos, multiseleccione los métodos utilizando las combinaciones de teclas del mandato Ctrl o Mayús y, a continuación, seleccione las propiedades a las que desea asignar los métodos.

- c. Pulse **Finalizar** para añadir los registros a la Base de datos de conocimientos de AppScan Source Security.
10. Si está añadiendo métodos como “Receptor (susceptible a la corrupción)” en la página 241:
  - a. Pulse **Siguiente** para continuar en la página **Asignar atributos de regla**.
  - b. Para cada método que haya añadido:
    - Seleccione el nivel **Gravedad** del impacto de vulnerabilidad: **Alto**, **Medio** o **Bajo**.
    - Seleccione el **Tipo de vulnerabilidad** a aplicar al método.

**Consejo:** Para añadir las mismas propiedades a varios métodos, multiseleccione los métodos utilizando las combinaciones de teclas del mandato Ctrl o Mayús y, a continuación, seleccione las propiedades a las que desea asignar los métodos.

- c. Pulse **Finalizar** para añadir los registros a la Base de datos de conocimientos de AppScan Source Security.
11. Si está añadiendo métodos como “Resultado sin rastreo” en la página 241:
  - a. Pulse **Siguiente** para continuar en la página **Asignar atributos de regla**.
  - b. Para cada método que haya añadido:
    - Seleccione el nivel **Gravedad** del impacto de vulnerabilidad: **Alto**, **Medio** o **Bajo**.
    - Seleccione la **Clasificación** para asignar al método: **Definitivo**, **Sospechoso** o **Configuración**.
    - Seleccione el **Tipo de vulnerabilidad** a aplicar al método.

**Consejo:** Para añadir las mismas propiedades a varios métodos, multiseleccione los métodos utilizando las combinaciones de teclas del mandato Ctrl o Mayús y, a continuación, seleccione las propiedades a las que desea asignar los métodos.

- c. Pulse **Finalizar** para añadir los registros a la Base de datos de conocimientos de AppScan Source Security.

## Atributos de reglas de probabilidad

Los atributos `Attribute.Likelihood.High` y `Attribute.Likelihood.Low` forman parte de las reglas predefinidas y se pueden utilizar al crear reglas personalizadas.

En AppScan Source, *probabilidad* representa la probabilidad o la oportunidad de que se pueda explotar un resultado de seguridad. AppScan Source toma la definición de probabilidad presente en [https://www.owasp.org/index.php/OWASP\\_Risk\\_Rating\\_Methodology#Step\\_2:\\_Factors\\_for\\_Estimating\\_Likelihood](https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology#Step_2:_Factors_for_Estimating_Likelihood), y la acota determinando la probabilidad en función de las propiedades de rastreo. Dado un conjunto de propiedades de rastreo (por ejemplo, nombre de API de origen, tipo de API de origen, tecnología de origen o mecanismo de origen), AppScan Source determinará la probabilidad de que un rastreo pueda o sea explotado mediante una vulnerabilidad específica en el futuro.

La probabilidad está unida al elemento de origen de un rastreo. Un origen es una entrada para el programa, como un archivo, una solicitud de servlet, una entrada de consola o un socket. En la mayoría de los orígenes de entrada, los datos devueltos son ilimitados en términos de contenido y longitud. Cuando se deselecta una entrada, se considera que está corrupta.

Algunos ejemplos de probabilidad incluyen:

- Dado un rastreo con un origen HTTP (por ejemplo, `Request.getQueryString`) y un receptor de script entre sitios (por ejemplo, `Response.write`), se ha determinado una probabilidad alta, aumentando así la confianza del resultado.
- Dado un rastreo con un origen de propiedad de sistema (por ejemplo, `getProperty`) y un receptor de script entre sitios (por ejemplo, `Response.write`), se ha determinado una probabilidad baja, disminuyendo así la confianza del resultado.

La probabilidad se utiliza para identificar resultados accionables de prioridad alta que deben seguir o que se deben arreglar inmediatamente. Está unida a orígenes altamente explotables de corrupción y puede proporcionarle un enfoque más preciso para clasificar resultados. La probabilidad se almacena como un atributo que está unido a un origen de corrupción, en la base de datos de vulnerabilidad de AppScan Source. La característica está disponible de forma predeterminada.

Hemos llevado a cabo una búsqueda exhaustiva para determinar el factor de probabilidad para los orígenes. Mediante el uso del Asistente de reglas personalizadas, puede añadir información de probabilidad a nuevos orígenes de corrupción que añade a la base de la regla. Esto mejorará la clasificación de resultados generados desde un escaneo y, a su vez, mejora la eficiencia del flujo de trabajo de asignación de prioridades global.

En el Asistente de reglas personalizadas, hay dos valores (**Alto** y **Bajo**) que puede establecer para la propiedad **Probabilidad**. Un valor de **Alto** significa que el origen es muy susceptible de corromperse. En otras palabras, la barrera para corromper la entrada al sistema es muy baja, lo que facilita que los atacantes envíen datos maliciosos de forma manual o automatizada. Un valor de **Bajo** significa que la barrera para introducir datos maliciosos mediante este origen es muy alta. Ello podría significar que, para que se introduzca corrupción en el origen, un atacante tendría que saber cómo funciona el sistema desde dentro y tener permisos para operar en la red de la víctima.

---

## Personalización del rastreo de entrada/salida a través del rastreo de AppScan Source

Algunas aplicaciones (en particular las aplicaciones web) necesitan el rastreo de entrada/salida para identificar vulnerabilidades de seguridad relacionadas con inyección por SQL, inyección por mandatos y script entre sitios. Mediante el rastreo de AppScan Source, puede especificar una rutina de validación que, cuando se use, elimine la notificación de cualquier vulnerabilidad. Las demás salidas se marcan como vulnerabilidades si la entrada no se ha validado.

Las rutinas de validación definidas por el usuario son rutinas que procesan datos de entrada y los convierten en seguros para que se pasen a rutinas de salida. Si una rutina de validación procesa datos de entrada antes de pasarlos a una rutina de salida, no existe ninguna vulnerabilidad de validación de entrada. Los desarrolladores pueden especificar sus propias rutinas de validación y codificación de entrada para trabajar con el rastreo.

---

## Personalización con reglas basadas en patrón

El escaneo basado en patrones de AppScan Source es un análisis del código fuente basado en criterios de búsqueda personalizados. El escaneo basado en patrones se parece a grep (grep busca uno o varios archivos para una serie de caracteres o patrón determinados). Los auditores o analistas de seguridad que realicen selecciones pueden utilizar el escaneo basada en patrones para buscar patrones específicos en determinadas aplicaciones o en un proyecto. Una vez se ha definido un patrón como tipo de vulnerabilidad, una escaneo del código fuente identifica el patrón como una vulnerabilidad. Cuando AppScan Source encuentra una coincidencia, el elemento aparece en la tabla de resultados. La biblioteca de reglas lista para su utilización de AppScan Source incluye conjuntos de reglas y reglas predefinidas (colecciones de reglas).

El escaneo basado en patrones busca una *expresión regular*. Una expresión regular, generalmente denominada patrón, es una serie que describe o compara un conjunto de series, en función de ciertas reglas de sintaxis. Especifique una búsqueda creando una regla. Una regla es similar a una regla personalizada que se añade a la Base de datos de conocimientos de AppScan Source Security en la vista Reglas personalizadas. Cuando se crea una regla, se define gravedad, clasificación, tipo de vulnerabilidad y otros criterios.

La “Vista Biblioteca de reglas de patrón” en la página 295 le permite crear nuevas reglas de patrón y conjuntos de reglas; y se puede modificar o eliminar reglas existentes. Utilice entonces la vista Propiedades para una aplicación seleccionada, la vista Propiedades para un proyecto seleccionado, o configuraciones de escaneo para aplicar las reglas de patrones y los conjuntos de reglas (también puede iniciar el cuadro de diálogo que le permite crear una regla nueva desde estas vistas). Para obtener más información sobre las reglas de aplicación y los conjuntos de reglas, consulte “Aplicación de reglas de patrón y de conjuntos de reglas” en la página 254.

Entre las reglas de patrón que se pueden crear se encuentran las siguientes:

- Coincidencias de patrones de nombre de archivo
- Una sola regla con varios patrones
- Reglas de ausencia

**Nota:** Debe tener el permiso **Gestionar patrones** para poder crear reglas de patrón o conjuntos de reglas, o para modificar y eliminar reglas personalizadas y conjuntos de reglas.

## Conjuntos de reglas de patrón

Un conjunto de reglas de patrón es una recopilación de reglas de patrón. Puede añadir nuevos conjuntos de reglas de patrón o puede modificar o eliminar los existentes. AppScan Source proporciona una serie de conjuntos de reglas de patrón específicas de cada lenguaje que puede elegir para aplicar a sus proyectos o aplicaciones (por ejemplo, podría desear aplicar el conjunto de reglas de patrón **Java** a sus proyectos **Java/JSP**).

La “Vista Biblioteca de reglas de patrón” en la página 295 le permite crear nuevas reglas de patrón y conjuntos de reglas; y se puede modificar o eliminar reglas existentes. Utilice entonces la vista **Propiedades** para una aplicación seleccionada, la vista **Propiedades** para un proyecto seleccionado, o configuraciones de escaneo para aplicar las reglas de patrones y los conjuntos de reglas (también puede iniciar el cuadro de diálogo que le permite crear una regla nueva desde estas vistas). Para obtener más información sobre las reglas de aplicación y los conjuntos de reglas, consulte “Aplicación de reglas de patrón y de conjuntos de reglas” en la página 254.

Algunos de los conjuntos de reglas de patrón que se suministran con AppScan Source no contienen ninguna regla. Puede añadir reglas que resulten adecuadas para la organización a dichos conjuntos de reglas. Estos conjuntos de reglas incluyen:

- ColdFusion
- JQuery
- JavaScript del lado del cliente
- Visual Basic 6
- MooTools

**Consejo:** En la vista Biblioteca de reglas de patrón, pulse con el botón derecho del ratón en un conjunto de reglas y seleccione **Propiedades** para abrir un cuadro de diálogo que muestra información sobre el conjunto de reglas. El cuadro de diálogo **Propiedades** del conjunto de reglas ofrece información como el número de reglas del conjunto de reglas de patrón y las relaciones padre/hijo con otros conjuntos de reglas. También le permite modificar el **Nombre de visualización** y los **Tipos de proyecto** del conjunto de reglas.

**Nota:** Debe tener el permiso **Gestionar patrones** para poder crear reglas de patrón o conjuntos de reglas, o para modificar y eliminar reglas personalizadas y conjuntos de reglas.

### Creación de un conjunto de reglas en la vista Biblioteca de reglas de patrón

Un conjunto de reglas de patrón es una recopilación de reglas de patrón. Para obtener más información sobre cómo crear un conjunto de reglas, siga las instrucciones de este tema.



## Antes de empezar

**Nota:** Debe tener el permiso **Gestionar patrones** para poder crear reglas de patrón o conjuntos de reglas, o para modificar y eliminar reglas personalizadas y conjuntos de reglas.

### Procedimiento

1. En la vista Biblioteca de reglas de patrón, pulse **Conjunto de reglas nuevas**.
2. En el cuadro de diálogo Conjunto de reglas nuevas, escriba un nombre para el conjunto de reglas en el campo **Nombre**.
3. Seleccione uno o varios tipos de proyectos a los que se aplicará el conjunto de reglas.
4. Pulse **Aceptar**.
5. El nuevo conjunto de reglas aparecerá en la lista de conjunto de reglas. Puede llenar el conjunto de reglas de una de estas formas:
  - a. Seleccione una o varias reglas en la sección de reglas de patrón y arrástrelas y suéltelas en el conjunto de reglas.
  - b. Seleccione una o varias reglas en la sección de reglas de patrón y, a continuación, pulse con el botón derecho del ratón en la selección y seleccione el elemento de menú **Añadir a conjunto de reglas**. En el cuadro de diálogo Elegir conjunto de reglas, seleccione el conjunto de reglas al que desea añadir la regla o reglas.

### Modificación y eliminación de conjuntos de reglas

Los conjuntos de reglas de patrón predeterminados y los conjuntos de reglas que ha creado se pueden modificar y eliminar en la vista Biblioteca de reglas de patrón.

**Nota:** Debe tener el permiso **Gestionar patrones** para poder crear reglas de patrón o conjuntos de reglas, o para modificar y eliminar reglas personalizadas y conjuntos de reglas.

### Modificación de un conjunto de reglas

Se pueden realizar las siguientes modificaciones en un conjunto de reglas:

- Puede añadir una regla a un conjunto de reglas existente siguiendo las instrucciones para llenar un nuevo conjunto de reglas de “Creación de un conjunto de reglas en la vista Biblioteca de reglas de patrón” en la página 248.
- Para eliminar una o varias reglas de un conjunto de reglas, seleccione la regla o las reglas a eliminar y, a continuación, realice una de estas acciones:
  - Pulse **Eliminar reglas del conjunto**.
  - Pulse con el botón derecho y seleccione **Eliminar reglas del conjunto**.
- Puede añadir un conjunto de reglas a otro conjunto de reglas de una de estas formas:
  - Seleccione un conjunto de reglas y arrástrelo y suéltelo en otro conjunto de reglas.
  - Pulse con el botón derecho en un conjunto de reglas y seleccione **Añadir conjunto de reglas como hijo** y, a continuación, en el cuadro de diálogo Elegir conjunto de reglas, seleccione el conjunto de reglas que desea añadir como conjunto de reglas padre.
- Puede modificar el **Nombre de visualización** y los **Tipos de proyectos** de un conjunto de reglas: Pulse con el botón derecho del ratón el conjunto de reglas y

seleccione **Propiedades** para abrir el recuadro de diálogo Propiedades del conjunto de reglas. En este recuadro de diálogo, puede editar el campo **Nombre de visualización**, o puede pulsar el campo **Tipos de proyecto** y el botón **Editar** para seleccionar uno o varios tipos de proyectos.

## Eliminación de un conjunto de reglas

Para eliminar un conjunto de reglas, selecciónelo y realice una de estas acciones:

- Pulse **Eliminar conjunto de reglas**.
- Pulse con el botón derecho del ratón y seleccione **Eliminar**.

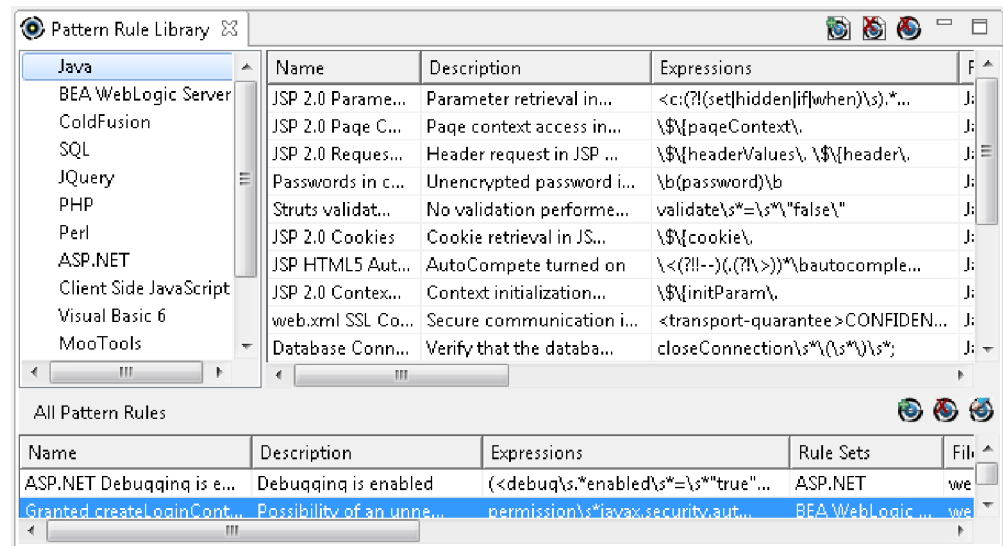
## Reglas de patrón

Las reglas de texto de AppScan Source pueden ser impresión de expresiones regulares globales ampliadas (Extended Global Regular Expressions Print, egrep), expresiones regulares globales (Global Regular Expressions, grep) o expresiones regulares de Perl. Estas expresiones regulares (expresiones que tienen valores de series que utilizan el conjunto completo de caracteres alfanuméricos y especiales) se comparan con las reglas.

| Carácter    | Descripción                                                  |
|-------------|--------------------------------------------------------------|
| ^           | Empieza por                                                  |
| \$          | termina por                                                  |
| \n, \t o \r | Nueva línea literal, tabulador, retorno de carro             |
| [xyz]       | Cualquiera de los caracteres listados                        |
| [^abx]      | Cualquier carácter excepto los listados                      |
| [a-fA-F0-9] | Cualquier carácter hexadecimal                               |
| .           | Cualquier carácter                                           |
|             | Cualquiera                                                   |
| \           | Cancelar significado del carácter especial<br>\\ \$ \^ \\ \? |

Las reglas de patrón se almacenan en una biblioteca global de reglas de patrón (en la base de datos de AppScan Source) y se pueden compartir entre proyectos y aplicaciones. Las reglas y los conjuntos de reglas también las pueden compartir todos los usuarios. Las reglas se añaden por referencia, lo que puede inhabilitar eliminando la referencia en el objeto asociado sin suprimir la regla subyacente.

Cree reglas en la vista Biblioteca de reglas de patrón, en el separador Propiedades de la vista Explorador, o en una configuración de escaneo. Al instalar AppScan Source, la vista Biblioteca de reglas de patrón mostrará las reglas proporcionadas por AppScan Source. En esta vista puede editar, suprimir o crear una regla.



**Importante:** Puede añadir o eliminar criterios de búsqueda, pero cada regla basada en patrones debe tener al menos un criterio de búsqueda.

## Búsqueda de patrones de texto

Dentro de un determinado archivo de origen, el escaneo basado en patrones busca patrones de texto en archivos por extensión, lo que permite realizar búsquedas en archivos de origen, archivos de configuración XML y otros archivos de texto.

Por ejemplo, puede crear una búsqueda de patrón para asegurarse de que no se codifiquen en la aplicación direcciones de correo electrónico equivocadas. En este caso, si desea asegurarse de que la aplicación no utilice direcciones de correo electrónico corporativas, podría buscar un patrón como por ejemplo `.*@mycompany.com`.

## Ejemplos

| Este patrón encuentra                                                     | Patrón                                                 |
|---------------------------------------------------------------------------|--------------------------------------------------------|
| Una dirección de correo electrónico                                       | <code>[A-Za-z]\.[A-Za-z]@[A-Za-z][A-Za-z]\.com</code>  |
| Todas las instancias del patrón, como por ejemplo <code>passWord =</code> | <code>[Pp][Aa][Ss][Ss][Ww][Oo][Rr][Dd]\W*=</code>      |
| Cualquier instancia del algoritmo hash MD5                                | <code>getInstance[[:space:]]*\([[:space:]]*"MD5</code> |

## Creación de una regla de patrón

Las reglas se pueden crear en la vista Biblioteca de reglas de patrón, en la vista Propiedades para un proyecto o aplicación, o en una configuración de escaneo.

### Antes de empezar

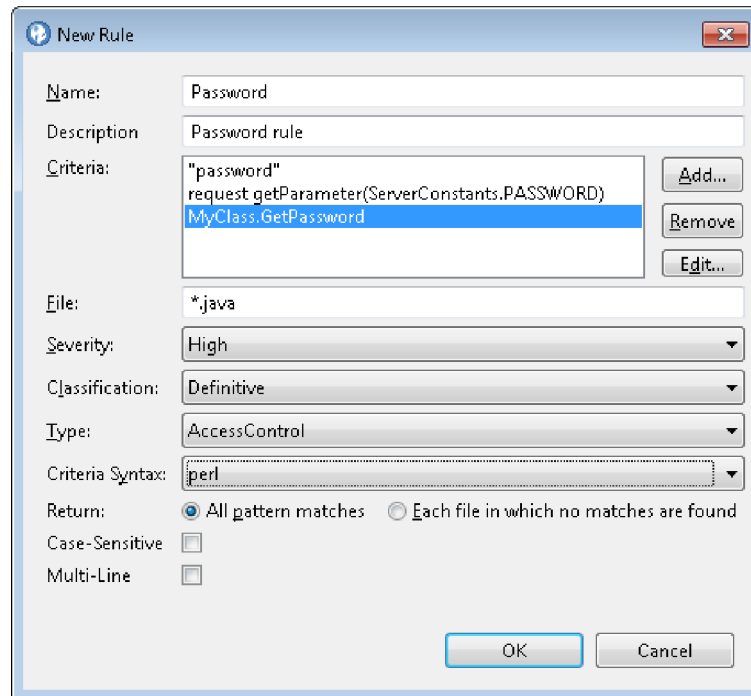
**Nota:** Debe tener el permiso **Gestionar patrones** para poder crear reglas de patrón o conjuntos de reglas, o para modificar y eliminar reglas personalizadas y conjuntos de reglas.

Las reglas se crean en el recuadro de diálogo Regla nueva:

- Para abrir este recuadro de diálogo en la vista Biblioteca de reglas de patrón, pulse **Regla nueva**.
- En una configuración de escaneo, seleccione el separador **Análisis de patrones** y, a continuación, seleccione el recuadro de selección **Análisis de patrones**. En la sección Reglas de patrón del separador, pulse **Añadir** para abrir el recuadro de diálogo Añadir reglas de patrón. En este recuadro de diálogo, pulse **Crear regla nueva** para abrir el recuadro de diálogo Regla nueva.
- Para abrir este recuadro de diálogo desde la vista Propiedades para un proyecto o aplicación seleccionado, seleccione el separador **Reglas y conjuntos de reglas** de la vista Propiedades, pulse **Añadir** o pulse con el botón derecho del ratón dentro de la sección Reglas y seleccione **Añadir**. Pulse **Regla nueva** en el recuadro de diálogo Elegir regla.

## Procedimiento

1. En el recuadro de diálogo Regla nueva, asigne un **Nombre** a la regla.
2. Opcional: Añada una **Descripción** para la regla.
3. Añada los **Criterios**. Pulse en **Añadir** y escriba la expresión regular para cada regla.
4. Identifique el tipo de archivo, como por ejemplo \*.java o \*.xml. Puede escribir cualquier tipo de archivo con o sin caracteres comodín.
5. Opcional: Seleccione la **Gravedad**:
  - **Alta**
  - **Media**
  - **Baja**
  - **Info**
6. Opcional: Seleccione la **Clasificación**:
  - **Definitivo**
  - **Sospechoso**
  - **Cobertura de escaneo**
7. Opcional: Seleccione el tipo de vulnerabilidad que hay que buscar en el escaneo. (Para ver más detalles sobre los tipos de vulnerabilidad, consulte la Base de datos de conocimientos de AppScan Source Security)



8. Opcional: Seleccione la sintaxis de criterios:

- **egrep**
- **grep**
- **perl**

9. Opcional: Identifique si los resultados devueltos incluyen **Todas las coincidencias de patrón** o **Archivos en los que no se han encontrado coincidencias**. Cuando no se encuentra ninguna coincidencia, el patrón es una regla de ausencia.

10. Opcional: Seleccione el recuadro de selección **Distinguir mayúsculas de minúsculas** si la coincidencia del patrón debe distinguir entre mayúsculas y minúsculas.

11. Opcional: Seleccione el recuadro de selección **Multilínea** si la regla debe coincidir con un patrón que abarca varias líneas.

12. Pulse en **Aceptar** para verificar que las expresiones regulares de la regla son válidas. Luego la regla se añade a la biblioteca de reglas de patrón.

## Modificación y eliminación de reglas de patrón

Las reglas de patrón que ha creado se pueden modificar y eliminar en la vista Biblioteca de reglas de patrón.

**Nota:** Debe tener el permiso **Gestionar patrones** para poder crear reglas de patrón o conjuntos de reglas, o para modificar y eliminar reglas personalizadas y conjuntos de reglas.

## Modificación de una regla

Para editar una regla, selecciónela y realice una de estas acciones:

- Pulse **Editar regla**.
- Pulse con el botón derecho y seleccione **Editar**.

Esto abre el recuadro de diálogo Editar regla, que le permite modificar cualquier valor excepto el nombre de la regla.

## Eliminación de una regla

Seleccione una o varias reglas y realice una de estas acciones:

- Pulse **Eliminar regla**.
- Pulse con el botón derecho del ratón y seleccione **Eliminar**.

## Aplicación de reglas de patrón y de conjuntos de reglas

Las reglas y los conjuntos de reglas se aplican en el nivel de proyecto o de aplicación en la vista Propiedades, o en una configuración de escaneo. Después de escanear aplicaciones o proyectos con reglas aplicadas, o de utilizar una configuración de escaneo que incluye reglas, los resultados de la búsqueda de reglas aparecerán en las vistas que contienen resultados.

### Aplicación de reglas y de conjuntos de reglas en una configuración de escaneo

Para habilitar el escaneo basado en patrones, seleccione el recuadro de selección **Análisis de patrones**. Cuando lo haga, se habilitarán las secciones **Conjuntos de reglas de patrón** y **Reglas de patrón**:

- Para añadir un conjunto de reglas, pulse **Añadir** en la sección **Conjuntos de reglas de patrón**. Esto abre el recuadro de diálogo Añadir conjuntos de reglas de patrón, que le permite seleccionar uno o varios conjuntos de reglas. Al seleccionar un conjunto de reglas, las reglas que contiene se mostrarán en el lado derecho del recuadro de diálogo, y los tipos de proyecto a los que se aplica el conjunto de reglas se listarán en el campo **Tipos de proyecto**. Pulse en **Aceptar** para añadir los conjuntos de reglas seleccionados.
- Para añadir una regla, pulse **Añadir** en la sección **Reglas de patrón**. Esto abre el recuadro de diálogo Añadir patrón, que le permite seleccionar una o varias reglas. También puede pulsar **Crear regla nueva** para crear una regla nueva (consulte “Creación de una regla de patrón” en la página 251). Si crea una regla nueva, se añadirá a la lista y se seleccionará. Tras seleccionar o crear reglas, pulse en **Aceptar** para añadirlas a la configuración de escaneo.

**Consejo:** En el recuadro de diálogo Añadir reglas de patrón, la ayuda emergente indica las expresiones utilizadas para cada regla.

### Aplicación de reglas y de conjuntos de reglas mediante la vista Propiedades

Seleccione el proyecto o la aplicación en la vista Explorador y, a continuación, realice las modificaciones que se muestran a continuación en el separador Reglas de patrón y conjuntos de reglas de su vista Propiedades. Después de especificar las reglas y los conjuntos de reglas que desea aplicar a la aplicación o proyecto, guarde las propiedades de la aplicación o proyecto. Los siguientes escaneos de la aplicación o proyecto incluirán las reglas.

- Para añadir un conjunto de reglas, pulse **Añadir** en la sección **Conjuntos de reglas**, o bien pulse con el botón derecho del ratón en la sección y seleccione **Añadir**. Esto abre el recuadro de diálogo Elegir regla, que le permite seleccionar un conjunto de reglas a añadir.

- Para eliminar un conjunto de reglas de modo que no se utilice durante escaneos de la aplicación o proyecto, selecciónelo y pulse **Eliminar** o pulse con el botón derecho del ratón el conjunto de reglas y seleccione **Eliminar**.
- Para añadir una regla, pulse **Añadir** en la sección **Reglas**, o bien pulse con el botón derecho del ratón en la sección y seleccione **Añadir**. Esto abre el recuadro de diálogo Elegir regla, que le permite seleccionar una regla a añadir. En este recuadro de diálogo, también puede pulsar **Nueva regla** para crear una regla nueva (consulte “Creación de una regla de patrón” en la página 251). Si crea una regla nueva, se añadirá a la lista y se seleccionará. Tras seleccionar o crear una regla, pulse **Aceptar** para añadirla.
- Para eliminar una regla de modo que no se utilice durante escaneos de la aplicación o proyecto, selecciónela y pulse **Eliminar** o pulse con el botón derecho del ratón la regla y seleccione **Eliminar**. También puede multiseleccionar varias reglas y eliminarlas utilizando estas acciones.

## Vista Configuración del escaneo

La vista Configuración del escaneo le permite crear configuraciones que puede utilizar al iniciar escaneos. También puede utilizar la vista para establecer una configuración de escaneo predeterminada. En una configuración de escaneo, puede especificar las reglas de origen que se utilizan durante un escaneo y puede incluir varios valores de escaneo. Los valores establecidos en una configuración de escaneo a menudo pueden mejorar los resultados del escaneo, y la posibilidad de guardar estos valores facilita el escaneo y permite ahorrar tiempo.

La vista Configuración del escaneo tiene estas secciones principales:

- “Gestión de la configuración de escaneo” en la página 119
- “Separador General” en la página 120
- “Separador Análisis de flujo corrupto” en la página 120
- “Separador Análisis de patrones” en la página 121

## Gestión de la configuración de escaneo

Utilice esta sección para seleccionar, añadir, eliminar, guardar y compartir configuraciones de escaneo, así como para establecer configuraciones de escaneo predeterminadas.

- Para crear una nueva configuración de escaneo, pulse **Nueva**. Después de completar los valores de la configuración de escaneo, pulse **Guardar** para guardar los cambios. Para establecer la configuración de escaneo como el valor predeterminado, pulse **Seleccionar como valor predeterminado** después de guardarla. Para obtener más información sobre cómo se utiliza la configuración de escaneo predeterminada, consulte “Escaneo de código fuente” en la página 109.
- Para trabajar con una configuración de escaneo existente, selecciónela en la lista:
  - Si modifica los valores de la configuración de escaneo, pulse **Guardar** para guardar los cambios (para descartar los cambios no deseados, cambie a otra configuración de escaneo y pulse **Descartar**).
  - Para eliminar la configuración de escaneo seleccionada, pulse **Suprimir**.
  - Para duplicar la configuración de escaneo, pulse **Duplicar**. Se creará una nueva configuración de escaneo basada en los valores de la configuración de escaneo original.
  - Para establecer la configuración de escaneo como el valor predeterminado, pulse **Seleccionar como valor predeterminado**. Para obtener más información

sobre cómo se utiliza la configuración de escaneo predeterminada, consulte “Escaneo de código fuente” en la página 109.

- Para compartir la configuración de escaneo con otras personas, pulse **Compartir**. La configuración de escaneo se guardará en base de datos de AppScan Source.

**Nota:** Para compartir configuraciones de escaneo, o para modificar o suprimir una configuración de escaneo compartida, debe tener permiso para **Gestionar configuraciones compartidas**. Para obtener información sobre cómo establecer permisos, consulte el manual *IBM Security AppScan Source Guía de instalación y administración*.

**Nota:** AppScan Source proporciona configuraciones de escaneo incorporadas. Estas no se pueden modificar ni eliminar. Si las selecciona en la lista, podrá duplicarlas o ver sus valores.

## Separador General

### Información básica

Esta sección permite nombrar configuraciones de escaneo y proporcionar descripciones.

### Filtros

En esta sección, puede elegir uno o varios filtros para aplicar al escaneo, siempre que se utilice la configuración de escaneo. Al seleccionar un filtro, puede elegir un AppScan Source filtro predefinido o un filtro compartido o uno que haya creado. Consulte “Gestión de las configuraciones de escaneo” en la página 113 para ver más detalles.

## Separador Análisis de flujo corrupto

### Análisis de flujo corrupto

Habilite y establezca el ámbito del análisis de flujo corrupto.

### Reglas de escaneo

Utilice esta sección para determinar qué reglas de origen se aplicarán en el escaneo.

Un origen es una entrada para el programa, como un archivo, una solicitud de servlet, una entrada de consola o un socket. Al excluir algunas reglas de origen, puede acelerar el escaneo y evitar la detección de vulnerabilidades debidas a entradas que no son de interés.

Las reglas se etiquetan con propiedades de reglas para indicar que están relacionadas con una determinada vulnerabilidad, mecanismo, atributo o tecnología. Estas propiedades se agrupan en conjuntos de reglas, que se corresponden con un conjunto común de reglas relacionadas. Puede limitar las reglas de origen incluidas en el escaneo mediante la especificación de conjuntos de reglas o propiedades de reglas individuales.

- Seleccione uno o varios tipos de vulnerabilidad (organizados por tipo en los conjuntos de reglas) que desee incluir en el escaneo:



- **Todo:** si selecciona esta opción, se detectarán las vulnerabilidades debidas a todos los orígenes de entrada soportados.
- **Entrada de usuario:** si selecciona esta opción, se detectarán las vulnerabilidades debidas a la entrada del usuario final.
- **Aplicaciones web:** si selecciona esta opción, se detectarán las vulnerabilidades debidas al riesgo de las aplicaciones web.
- **Registro y manejo de errores:** si selecciona esta opción, se detectarán las vulnerabilidades debidas a los mecanismos de registro y manejo de errores.
- **Entorno:** si selecciona esta opción, se detectarán las vulnerabilidades debidas a los archivos de configuración, los archivos del entorno del sistema y los archivos de propiedades.
- **Sistemas externos:** si selecciona esta opción, se detectarán las vulnerabilidades debidas a las entidades externas.
- **Almacén de datos:** si selecciona esta opción, se detectarán las vulnerabilidades debidas a los almacenes de datos (por ejemplo, las bases de datos y la memoria caché).
- **Elementos poco usuales:** si selecciona esta opción, se detectarán las vulnerabilidades debidas a las rutinas que no forman parte normalmente de una aplicación de producción.
- **Sistema de archivos:** si selecciona esta opción, se detectarán las vulnerabilidades debidas a los sistemas de archivos.
- **Datos confidenciales:** si selecciona esta opción, se detectarán las vulnerabilidades debidas a los datos confidenciales.

El texto flotante describe cada conjunto de reglas de esta sección.

- Seleccione las propiedades de las reglas de escaneo individuales que desee incluir en el escaneo: pulse **Descartar los conjuntos de reglas seleccionados y permitir seleccionar propiedades de regla individuales**. Esto abre el cuadro de diálogo Seleccionar propiedades de reglas, que le permite seleccionar las propiedades de la regla individual. Si se rellena este cuadro de diálogo, se descartarán los conjuntos de reglas que se hayan seleccionado. Las reglas de escaneo que tienen seleccionadas propiedades de regla se utilizarán para el escaneo.

## Valores avanzados

Esta sección está especialmente indicada para usuarios avanzados. Contiene una amplia variedad de valores que pueden mejorar los resultados del escaneo. El texto flotante describe cada valor de esta sección.

## Separador Análisis de patrones

### análisis de patrón

Utilice esta sección para habilitar el escaneo basado en patrones cuando se utilice la configuración de escaneo. El escaneo basado en patrones es un análisis del código fuente basado en criterios de búsqueda personalizados.

### Conjuntos de reglas de patrón y Reglas de patrón

Utilice estas secciones para añadir reglas y conjuntos de reglas a utilizar durante el análisis de patrones. Consulte los apartados “Personalización con reglas basadas en patrón” en la página 247 y “Gestión de las configuraciones de escaneo” en la página 113 para obtener más información.

## Vista Propiedades: aplicación seleccionada

En esta vista puede configurar atributos para la aplicación seleccionada. Los atributos de la aplicación dependen de los atributos globales creados con anterioridad.

- “Visión general”
- “Exclusiones y filtros”
- “Reglas y conjuntos de reglas”
- “Resultados modificados” en la página 259
- “Resultados personalizados” en la página 259

### Visión general

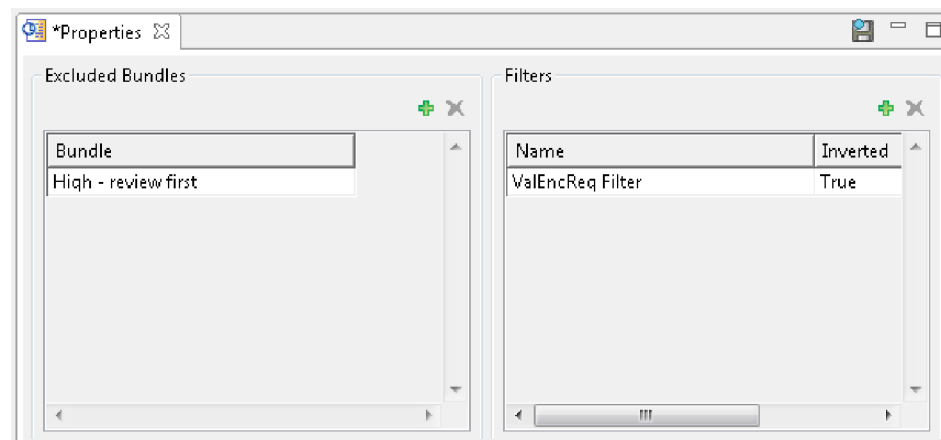
El separador Visión general muestra:

- Nombre de aplicación. La aplicación se puede renombrar especificando un nombre nuevo en el campo.
- Atributos de aplicación

### Exclusiones y filtros

Este separador permite especificar filtros existentes a la aplicación seleccionada, y la forma en que desea aplicar los filtros (un filtro se puede aplicar de forma directa o de forma inversa). En el separador, también puede gestionar los paquetes que excluyen resultados de escaneo. Consulte Capítulo 5, “Selección y análisis”, en la página 145 para obtener información sobre los filtros y “Aplicación de filtros globalmente” en la página 168 para obtener más detalles sobre cómo aplicarlos globalmente.

Los resultados excluidos y filtrados no aparecen en los resultados o factor del escaneo en métricas de la aplicación o del proyecto.



### Reglas y conjuntos de reglas

Cuando selecciona una aplicación en la vista Explorador, el separador Reglas de patrón y conjuntos de reglas de la vista Propiedades le permite añadir reglas de patrón y conjuntos de reglas que se aplicarán al escanear la aplicación. Si utiliza un escaneo basado en patrón, busca patrones de texto que desea que aparezcan como resultados. Las reglas individuales y los conjuntos de reglas se pueden aplicar a las aplicaciones y a los proyectos. Consulte “Personalización con reglas basadas en

patrón” en la página 247 para obtener información sobre el análisis basado en patrones y “Aplicación de reglas de patrón y de conjuntos de reglas” en la página 254 para obtener más información sobre cómo aplicar reglas y conjuntos de reglas en la vista Propiedades.

## Resultados modificados

En el separador Resultados modificados puede ver, editar o suprimir cualquier resultado anteriormente modificado o modificar un resultado existente. Los *resultados modificados* son resultados con el tipo de vulnerabilidad, gravedad, clasificación o notas alterados.

## Resultados personalizados

En el separador Resultados personalizados puede ver, añadir, editar o suprimir resultados personalizados. Consulte “Resultados personalizados” en la página 183 para obtener más información.

## Vista Propiedades: proyecto seleccionado

En esta modalidad de la vista Propiedades, puede configurar parámetros para el proyecto seleccionado. Los atributos del proyecto dependen de los atributos globales creados previamente. Las propiedades varían en función del proyecto seleccionado.

- “Separador visión general del proyecto seleccionado”
- “Filtros” en la página 261
- “Reglas de patrón y Conjuntos de reglas” en la página 261
- “Extensiones de archivo” en la página 261
- “Orígenes” en la página 262
- “Dependencias del proyecto JavaServer Page (JSP)” en la página 263
- “Dependencias del proyecto” en la página 263
- “Compilación” en la página 263
- “Optimizaciones” en la página 264
- “Separador Precompilar (solo ASP.NET)” en la página 264

## Separador visión general del proyecto seleccionado

El separador Visión general muestra:

- **Nombre** del proyecto. El proyecto se puede renombrar especificando un nombre nuevo en el campo.
- Nombre de **archivo** y vía de acceso del proyecto
- **Tipo de proyecto**
- Configuración: Esta sección visualiza la configuración de destino. Para proyectos .NET y C++, esta sección visualiza la configuración de destino que se ha guardado en el separador Dependencias del proyecto. Con todos los otros tipos de proyecto, esta sección visualiza **Predeterminado**.
- Opción de filtro: seleccione **Filtrar resultados contenidos en fuentes externas** para filtrar los resultados descubiertos en archivos que no son archivos de origen del proyecto escaneado. Esta opción reduce el ruido para los proyectos cuando los resultados se notifican en archivos temporales o generados por el compilador como, por ejemplo, ASP.NET.
- Opciones de memoria caché de análisis de vulnerabilidad: si está refinando el asesoramiento de una base de código escaneando iterativamente y añadiendo

reglas personalizadas y luego volviendo a escanear sin cambiar el código fuente, puede reducir significativamente el tiempo de escaneo si establece las propiedades del proyecto de modo que utilice una caché de análisis de vulnerabilidad. Para ello, marque el cuadro de selección **Habilitar memoria caché de análisis de vulnerabilidad** en las propiedades del proyecto. La primera vez que escanee el proyecto tras marcar este cuadro de selección, se creará una memoria caché de análisis de vulnerabilidad. Para cada siguiente escaneo del proyecto, se utilizará la memoria caché de análisis de vulnerabilidad y se reducirá el tiempo de escaneo.

Para borrar la caché de análisis de vulnerabilidad, y la caché que se crea cuando se ha habilitado el análisis incremental de Java, pulse **Borrar memoria caché**. La próxima vez que escanee un proyecto, tendrá lugar un escaneo completo y se creará una nueva caché de análisis de vulnerabilidad. Es posible que desee borrar la memoria caché si:

- El código fuente del proyecto se ha modificado desde el último escaneo.
- Ha realizado cambios en la configuración del proyecto, como por ejemplo añadir o suprimir archivos de origen.
- Ha cambiado las opciones de configuración del código fuente. Por ejemplo, puede que desee borrar la memoria caché si está escaneando Java y la vía de acceso de clase ha cambiado, o si está escaneando C o C++ y ha modificado la vía de acceso de inclusión o las definiciones de preprocesador.
- Ha habilitado el análisis incremental de Java y desea ejecutar un escaneo completo o se presentan problemas que pueden solucionarse borrando la caché. Consulte el apartado “Análisis incremental para Java” en la página 122 para obtener más información.

**Nota:** También puede borrar la memoria caché de análisis de vulnerabilidad marcando el cuadro de selección **Borrar memoria caché** al crear reglas personalizadas en el Asistente de reglas personalizadas.

- **Análisis de la cadena:** el análisis de la cadena supervisa la manipulación de cadenas en proyectos Java o Microsoft .NET. Proporciona la detección automática de rutinas de saneamiento y validación. Con esta detección se pueden reducir los falsos positivos y negativos. Marque el cuadro de selección **Habilitar análisis de la cadena para encontrar funciones validador/saneador** para habilitar el análisis de la cadena. El cuadro de selección **Aplicar las reglas importadas al ámbito global** determina si las rutinas de saneamiento o validación descubiertas se deben aplicar a un único proyecto o a nivel general (a todos los proyectos).

**Nota:** La aplicación del análisis de cadena puede ralentizar un escaneo. Por lo tanto, se recomienda que solo se aplique tras cambios en el código y luego se inhabilite para los siguientes escaneos. Además, las rutinas descubiertas se pueden ver como *sugerencias* y los auditores las pueden revisar. Estas rutinas se pueden ver en la vista Reglas personalizadas.

- **Codificación del archivo:** la codificación de caracteres de los archivos del proyecto debe establecerse de modo que AppScan Source pueda leer los archivos correctamente (y, por ejemplo, mostrarlos correctamente en la vista de origen).

**Nota:** La codificación del archivo predeterminado para proyectos AppScan Source es **ISO-8859-1**. La codificación de archivos predeterminada se puede cambiar en la página de preferencias generales.

## Filtros

Este separador permite especificar filtros existentes para el proyecto seleccionado, y la forma en que desea aplicar los filtros (un filtro se puede aplicar de forma directa o de forma inversa). Consulte Capítulo 5, “Selección y análisis”, en la página 145 para obtener información sobre los filtros y “Aplicación de filtros globalmente” en la página 168 para obtener más detalles sobre cómo aplicarlos globalmente.

## Reglas de patrón y Conjuntos de reglas

Cuando selecciona un proyecto en la vista Explorador, el separador Reglas de patrón y Conjuntos de reglas de la vista Propiedades le permitirá añadir reglas de patrón y conjuntos de reglas que se aplicarán al escanear el proyecto. Si utiliza un escaneo basado en patrón, busca patrones de texto que desea que aparezcan como resultados. Las reglas individuales y los conjuntos de reglas se pueden aplicar a las aplicaciones y a los proyectos. Consulte “Personalización con reglas basadas en patrón” en la página 247 para obtener información sobre el análisis basado en patrones y “Aplicación de reglas de patrón y de conjuntos de reglas” en la página 254 para obtener más información sobre cómo aplicar reglas y conjuntos de reglas en la vista Propiedades.

## Extensiones de archivo

Este separador sirve para configurar o añadir extensiones de archivo válidas para el proyecto, para excluir archivos de los escaneos y para especificar extensiones como archivos web.

La sección **Extensiones de archivo** muestra una lista de las extensiones que se han establecido de forma global en la página de preferencias “Extensiones de archivo de proyecto” en la página 107 para el tipo de proyecto actual (las extensiones de archivo se pueden elegir para un tipo de proyecto diferente utilizando el menú **Conjunto de extensiones de archivo**). Si desea excluir una extensión de los escaneos del proyecto actual, selecciónela en la lista y pulse **Extensión excluida**. Esto hace que la extensión aparezca listada en la sección **Extensiones excluidas** del separador.

Para añadir una extensión adicional al proyecto, seleccione **Añadir extensión** en la sección **Extensiones adicionales** y, a continuación, especifique la extensión del archivo e indique si los archivos con la extensión se deben escanear, considerar como un archivo web o si se deben excluir.

Tabla 22. Valores de extensión de archivo

| Valor                      | Descripción                                                                                                                                            | Ejemplos de utilización                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Escanear o Asesorar</b> | Incluir archivos con la extensión indicada en los análisis completos.                                                                                  | <ul style="list-style-type: none"> <li>• Si se crea una extensión .xxx para proyectos Java y se marca como <b>Escanear</b> o <b>Asesorar</b>, los archivos que tengan esta extensión se compilarán y escanearán.</li> <li>• Un archivo puede ser parte de un proyecto y no ser marcado como <b>Escanear</b> o <b>Asesorar</b> si no se debe compilar ni escanear (como por ejemplo, archivos de cabecera en C++). Estos archivos se deberían incluir en el proyectos, y se debería buscar en ellos durante el análisis basado en patrones.</li> </ul> |
| <b>Archivo web</b>         | Marca los archivos con la extensión indicada para la compilación de JSP. Este valor permite que AppScan Source separe orígenes web de orígenes no web. | Si se crea una extensión .yyy para proyectos Java y se marca como un <b>Archivo web</b> , los archivos que tengan esta extensión se organizarán como orígenes web en los proyectos. Cuando AppScan Source prepare el análisis, estos archivos serán precompilados en clases para ser analizados.                                                                                                                                                                                                                                                      |
| <b>Excluir</b>             | No crear archivos de origen en el proyecto para archivos con la extensión indicada. No se escanearán los archivos con esta extensión.                  | Cree una extensión .zzz para los archivos que son necesarios para la compilación de proyectos, pero que no se necesitan incluir en el análisis.                                                                                                                                                                                                                                                                                                                                                                                                       |

## Orígenes

Especifique los orígenes que se incluirán en el escaneo.

- Directorio de trabajo: la ubicación del archivo de proyecto de AppScan Source (ppf) y la base para todas las vías de acceso relativas.
- **Añadir raíz de origen** y **Elimina raíz de origen**: el separador Orígenes muestra las propiedades establecidas para el proyecto desde el Asistente de configuración de proyecto o definidas en el archivo ppf importado.  
**Eliminar raíz de origen** sólo está disponible cuando se selecciona el icono **Raíz de origen**. Se utiliza para eliminar el directorio raíz de código de origen.
- Encontrar raíces del origen (solo proyectos Java): dejar que AppScan Source for Analysis busque automáticamente todas las raíces de origen válidas.
- Los archivos de proyecto se listan bajo el icono **Raíz de origen**. Los archivos que se excluyen del escaneo tienen un icono de archivo rojo (si se pulsa con el botón derecho del ratón sobre un archivo excluido, su menú tiene **Excluir** inhabilitado e **Incluir** habilitado). Para excluir un archivo incluido, pulse con el botón

derecho del ratón sobre dicho archivo y elija **Excluir** en el menú. Para incluir un archivo excluido, pulse con el botón derecho del ratón sobre dicho archivo y elija **Incluir** en el menú.

## Dependencias del proyecto JavaServer Page (JSP)

El separador Dependencias del proyecto JSP muestra las propiedades establecidas para el proyecto JSP especificado.

- Contiene contenido (JSP) web: identifica si el proyecto es una aplicación web que contiene JavaServer Pages.
- Raíz de contexto web: un archivo WAR o un directorio que contiene el directorio WEB-INF. La raíz de contexto web debe ser la raíz de una aplicación web válida.
- Compilador de JSP: Tomcat 7, listo para utilizar, es el valor de compilador JSP predeterminado (el compilador JSP predeterminado se puede modificar en la página de preferencias de Java y JSP). Para conocer los compiladores a los que AppScan Source da soporte, consulte <http://www.ibm.com/support/docview.wss?uid=swg27027486>.

La instalación de AppScan Source incluye Apache Tomcat Versiones 7 y 8. Si las páginas de preferencias de **Tomcat 7** y **Tomcat 8** no están configuradas, AppScan Source compilará los archivos JSP mediante el compilador Tomcat JSP proporcionado que actualmente está marcado como predeterminado. Si desea utilizar un compilador Tomcat soportado externo, utilice la página de preferencias de Tomcat para apuntar a la instalación local de Tomcat.

Si utiliza un servidor de aplicaciones Oracle WebLogic Server o WebSphere Application Server, debe configurar la página de preferencias correspondiente para que apunte a la instalación local del servidor de aplicaciones a fin de que se pueda utilizar para la compilación de JSP durante el análisis. Si aún no ha finalizado esta configuración, se le solicitará mediante un mensaje el que lo haga cuando se seleccione el compilador JSP. Si pulsa **Sí** en el mensaje, se le llevará a la página de preferencias adecuada. Si pulsa **No**, un enlace de aviso aparecerá junto a la selección del compilador JSP (siguiendo dicho enlace se abrirá la página de preferencias).

## Dependencias del proyecto

El separador Dependencias del proyecto muestra propiedades del proyecto. Los valores de configuración en este separador varían según el lenguaje, por ejemplo:

- **Opciones** permite seleccionar los parámetros del compilador necesarios adicionales.
- Los valores de JDK son específicos de Java.
- Las definiciones de preprocesador son específicas del código C/C++. Al especificar definiciones de preprocesador, no incluya la opción -D del compilador (por ejemplo, especifique a=definition1 en lugar de -Da=definition1). Al especificar varios destinos, utilice una lista delimitada por puntos y comas.
- La configuración de destino sólo está disponible proyectos .NET y C++.

## Compilación

- Opciones: parámetros necesarios del compilador adicionales para la configuración del proyecto.
- Utilizar JDK: identificar el JDK utilizado para la compilación del proyecto, tal como está configurado en Preferencias. Consulte Capítulo 3, "Preferencias", en la página 93.

Los proyectos Java pueden hacer referencia a una ubicación local de Java Development Kit (JDK). Cuando los proyectos se mueven al servidor, es posible que la vía de acceso de JDK deje de ser válida. Para transferir proyectos locales al servidor, debe identificar la vía de acceso de JDK predeterminada para cada proyecto que especifica un JDK con nombre.

**Nota:** El compilador predeterminado, listo para utilizar, para los proyectos JSP es Tomcat 7, y necesita Java Versión 1.6 o superior. Si se mantiene **Tomcat 7** como predeterminado, utilizar un JDK anterior provocará errores de compilación durante los escaneos.

- Validar: **Validar** asegura que las dependencias del proyecto estén correctamente configuradas. Comprueba los proyectos Java para ver si hay conflictos de configuración entre los orígenes y la vía de acceso de clase y si existen errores de compilación. **Existe un conflicto** si una clase de una vía de acceso de clase está duplicada en una raíz de origen. (Si existe un conflicto, modifique la vía de acceso de clase para eliminar la clase conflictiva.)

Después de comprobar si existen conflictos, **Validar** determina si el proyecto se compila y notifica cualquier error de compilación.

### Optimizaciones

- **Clases precompiladas:** utilice archivos de clases precompiladas Java o JSP en lugar de realizar la compilación durante el escaneo. Si está seleccionada, esta opción inhabilita las opciones de organización de orígenes.
- Organizar archivos de origen para minimizar los efectos de errores de compilación: controla si AppScan Source copia los orígenes en el directorio de organización.

**Corregir para que los paquetes no coincidan con la estructura de directorio** requiere que la compilación de Java abra cada archivo de origen.

**Limpiar el área de transferencia entre cada escaneo** aumenta el rendimiento entre escaneos.

### Separador Precompilar (solo ASP.NET)

La precompilación se consigue realizando una solicitud HTTP a una página especial (precompile.axd de forma predeterminada) del sitio web. Esta página la procesa un manejador de HTTP especial especificado en el archivo web.config. Este manejador compila todo el sitio, incluidos los archivos client.aspx, en el directorio de archivos ASP.NET temporal del directorio del sistema .NET, donde todos se escanean.

Para escanear ASP.NET 1.1, debe instrumentar el sitio web de modo que dicho sitio compile y genere información de depuración. Por lo tanto, el hecho de que un sitio web compile y genere información de depuración constituye, por sí mismo, una vulnerabilidad de seguridad. Puede pasar por alto tranquilamente esta vulnerabilidad puesto que el escaneo lo requiere. Sin embargo, asegúrese de que la aplicación desplegada no se compile con debug=true en web.config.

Para precompilar un sitio web ASP.NET 1.1, añada este elemento como hijo al elemento <system.web> en el archivo web.config:

```
<httpHandlers><add verb="*" path="precompile.axd"
type="System.Web.Handlers.BatchHandler"/></httpHandlers>
```

También debe establecer debug=true en el elemento de compilación. Por ejemplo:



```

<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <system.web>
    <httpHandlers><add verb="*" path="precompile.axd"
      type="System.Web.Handlers.BatchHandler"/>
    </httpHandlers>
    <compilation
      defaultLanguage="c#"
      debug="true"
    />
  </system.web>
</configuration>
...

```

Este elemento especifica al sitio web que la página `precompile.axd` será manejada por la clase .Net especial `System.Web.Handlers.BatchHandler`. Esta clase precompila el contenido del sitio web en el directorio de archivos ASP.NET temporal.

- Sitio web: destino de la solicitud para precompilar el sitio. La ubicación predeterminada es `precompile.axd`. `Precompile.axd` es un archivo virtual y se correlaciona con el archivo especificado en el archivo `web.config`.
- Directorio de salida: el directorio de destino de la precompilación. AppScan Source busca la salida en este directorio.
- Precompilar el sitio web ASP.NET: AppScan Source precompila y escanea automáticamente la salida precompilada durante un escaneo.
- Detener escaneo si falla la precompilación: si se selecciona **Precompilar el sitio web ASP.NET** y **Detener escaneo si falla la precompilación**, un escaneo se detiene si la precompilación falla. De lo contrario, el escaneo continúa únicamente en la salida primaria del sitio web.
- Compilar ahora: probar que la precompilación, basada en los valores actuales, se realiza correctamente antes de realizar el escaneo. La salida de la compilación se muestra en el panel Salida de la precompilación.
- Ensamblados adicionales: para cualquier tipo de proyecto .NET, especifique los ensamblados adicionales que desea escanear.
- Preferencias del proyecto: lista de los directorios en los que hay que buscar ensamblados a los que se hace referencia en proyectos de ensamblado .NET y proyectos .NET existentes.



---

## Capítulo 11. Ampliación de la infraestructura de importación del servidor de aplicaciones

AppScan Source permite importar aplicaciones Java desde Apache Tomcat y WebSphere Application Server Liberty Profile. Puede importar aplicaciones Java desde otros servidores de aplicaciones ampliando la infraestructura de importación del servidor de aplicaciones, como se describe en este tema.

### Acerca de esta tarea

La infraestructura de importación del servidor de aplicaciones incluye documentación de la API que no está disponible en formato PDF. Si está accediendo a este tema de ayuda en formato PDF de Adobe, solo puede acceder a la documentación de la API iniciando la ayuda en línea de AppScan Source for Analysis y navegando a las secciones **Ampliación de la funcionalidad del producto > Ampliación de la infraestructura de importación del servidor de aplicaciones > Clases y métodos de la API de ampliación de la importación del servidor de aplicaciones** o puede localizar la sección de ayuda en <http://www.ibm.com/support/knowledgecenter/SSS9LM/welcome>.

Para ampliar la infraestructura de importación del servidor de aplicaciones, siga los pasos siguientes. En estos pasos realizará las acciones siguientes:

- Configurar un entorno de desarrollo integrado de Eclipse
- Crear un nuevo plugin en Eclipse
- Establecer las dependencias necesarias en el plugin creado recientemente
- En el plugin, defina una extensión para su servidor de aplicaciones
- Probar el plugin
- Habilitar el plugin para AppScan Source for Analysis

### Procedimiento

1. Configure un entorno de desarrollo integrado de Eclipse para las dependencias necesarias para la infraestructura de importación del servidor de aplicaciones de AppScan Source:
  - a. En Eclipse, seleccione **Ventana > Preferencias** en el menú principal.
  - b. En el recuadro de diálogo Preferencias, expanda **Desarrollo de plugins** y, a continuación, seleccione **Plataforma de destino**.
  - c. En la página de preferencias de Plataforma de destino, pulse **Añadir** para crear una nueva definición de destino.
  - d. En la página del asistente de Definición de destino, seleccione **Nada: Iniciar con una definición de destino vacía** y, a continuación, pulse **Siguiente**.
  - e. En la página del asistente de Contenido de destino, escriba un nombre para el destino en el campo **Nombre** y, a continuación, pulse **Añadir** para añadir su directorio de instalación de AppScan Source (consulte “Instalación y ubicaciones de archivo de datos de usuario” en la página 335).
  - f. Opcional: Seleccione **Mostrar contenido de ubicación** para verificar qué plugins están disponibles.
  - g. Pulse **Finalizar**.

- h. En la página de preferencias de Plataforma de destino, seleccione la plataforma que acaba de crear y pulse **Aplicar**. A continuación pulse **Aceptar**.
2. Cree un nuevo plugin en Eclipse:
  - a. Seleccione **Archivo > Nuevo proyecto** en el menú principal para abrir el asistente de Nuevo proyecto.
  - b. En la página Seleccionar un asistente, seleccione **Proyecto de plugin** y, a continuación, pulse **Siguiente**.
  - c. En la página Proyecto de plugin, escriba un nombre para el plugin en el campo **Nombre de proyecto** (este tema de ayuda utilizará `com.example.appserverimporter` como ejemplo) y, a continuación, pulse **Siguiente**.
  - d. En la página Contenido, deseccione **Generar un activador, una clase Java que controla el ciclo de vida del plugin** y, a continuación, pulse **Finalizar**.
3. En el plugin que acaba de crear, establezca las dependencias necesarias:
  - a. Abra `META-INF\MANIFEST.MF` y, a continuación, seleccione el separador **Dependencias**.
  - b. En la sección **Plug-ins necesarios** del editor:
    - Pulse **Añadir** y, a continuación, añada `com.ouncelabs.core.appserverimporter` y `org.eclipse.core.runtime`.
    - Seleccione el plugin `com.ouncelabs.core.appserverimporter` que se acaba de añadir y pulse **Propiedades**. En las propiedades del plugin, elimine las entradas de los campos **Versión mínima** y **Versión máxima** y, a continuación, pulse **Aceptar**.
    - Repita el paso anterior para el plugin `org.eclipse.core.runtime`.
  - c. Seleccione **Archivo > Guardar** en el menú principal para guardar todos los cambios realizados en el editor.
  - d. En el paso siguiente definirá una extensión para su servidor de aplicaciones. En dicho paso, continuará trabajando en el editor `META-INF\MANIFEST.MF`.
4. Defina una extensión de importador para el servidor de aplicaciones, siguiendo estos pasos:
  - a. Seleccione el separador **Extensiones**, a continuación, pulse **Añadir** para añadir `com.ouncelabs.appserver` y, a continuación, seleccione **Archivo > Guardar** en el menú principal.
  - b. Seleccione el separador **plugin.xml**. Su contenido deberá ser similar al siguiente:
 

```
<?xml version="1.0" encoding="UTF-8"?>
<?eclipse version="3.4"?>
<plugin>
  <extension
    point="com.ouncelabs.appserver">
  </extension>
</plugin>
```

Complete la definición de la extensión editando lo siguiente. Por ejemplo:

```
<?xml version="1.0" encoding="UTF-8"?>
<?eclipse version="3.4"?>
<plugin>
  <extension
    point="com.ouncelabs.appserver">
    <importer
      class="com.example.appserverimporter.MyAppServerImporter"
```

```

        id="com.example.appserverimporter.myapplication"
        name="My App Server">
    </importer> </extension>
</plugin>

```

- c. Seleccione **Archivo > Guardar** en el menú principal para guardar los cambios realizados en **plugin.xml**.
5. Cree la clase de importador (en este ejemplo, `com.example.appserverimporter.MyAppServerImporter`) para definir el comportamiento del nuevo importador del servidor de aplicaciones. Esta clase debe ampliar la implementación base de la infraestructura de `BaseAppServerImporter`, para la interfaz de `AppServerImporter`. En esta clase:
  - a. Implemente `AppServerImporter.importAppServer(String)`. Esto lo utiliza la infraestructura para determinar qué proyectos Java EE se han de importar y dónde están ubicados. Generalmente, para cada proyecto solo son necesarios el nombre y la vía de acceso del proyecto Java EE. Si se crean proyectos EAR, los proyectos Java EE contenidos se ocultarán cuando seleccione proyectos en la interfaz de usuarios de AppScan Source. En este caso, se importará todo el EAR. De lo contrario, se listarán todos los proyectos para que se seleccionen individualmente.  
Se recomienda utilizar estos métodos, siempre que resulte aplicable:
    - `BaseAppServerImporter.processDropInsFolder(AppServerProfile, File)`
    - `BaseAppServerImporter.processEARFile(AppServerProfile, File)`
  - b. Implemente `AppServerImporter.isValidLocation(String)`. Esto se utiliza para detectar el tipo de servidor, en función del directorio de instalación concreto.
  - c. Opcional: Altere temporalmente `BaseAppServerImporter.getJSPCompilerType()`. Este método devuelve el compilador JSP que se ha de utilizar para el proyecto AppScan Source. Si no se lleva a cabo, la implementación base devuelve nulo y se utiliza el compilador JSP predeterminado.
6. Opcional: Como opción avanzada, puede personalizar la compilación JSP para utilizar un compilador JSP precompilado (la compilación JSP tendrá lugar antes o durante el periodo de importación):
  - a. Altere temporalmente `BaseAppServerImporter.getJSPCompilerType()` para que devuelva `JSPCompilerType.PRECOMPILED`.
  - b. Altere temporalmente `BaseAppServerImporter.getJSPCompilerType()` para invocar JMX, la API Java, los scripts externos para compilar los archivos JSP, o simplemente copie los archivos de clases en el directorio de transición del proyecto de AppScan Source. Utilice `Application.getStagingDirectory(Project)` para obtener el directorio de transición.
  - c. Altere temporalmente `BaseAppServerImporter.createJSPCompilerSupport()` para que se devuelva una extensión personalizada de `JSPCompilerSupport`. Esto se utiliza para que persista la correlación entre los archivos JSP y los archivos de clases generados, y para su validación después de la compilación de JSP.
  - d. Altere temporalmente `BaseAppServerImporter.createClasspathProvider()` para que se devuelva una implementación personalizada de `AppServerClasspathProvider`. Esta clase es necesaria para compilar cualquier archivo Java o JSP que tenga dependencias con las bibliotecas del servidor. La clase debe ampliar `BaseAppServerClasspathProvider`. Tenga en cuenta que `BaseAppServerClasspathProvider.installDirectory` ya estará

establecido en el directorio de instalación para el servidor de aplicaciones cuando se invoca `getClasspathEntries()`.

7. Pruebe el plugin realizando estos pasos:
  - a. Seleccione **Ejecutar > Ejecutar configuraciones** en el menú principal (o **Ejecutar > Depurar** si desea realizar la prueba en modalidad de depuración).
  - b. Cree una nueva configuración de **Aplicación Eclipse**.
    - Vaya al separador **Principal** de la nueva configuración. En la sección **Programa a ejecutar**, seleccione **Ejecutar un producto** y, a continuación, establézcalo para ejecutar **com.ouncelabs.osa.rcp.product**.
    - Vaya al separador **Argumentos**. En la sección **Directorio de trabajo**, seleccione **Otros** y, a continuación, especifique el directorio de datos de AppScan Source en el campo (consulte “Instalación y ubicaciones de archivo de datos de usuario” en la página 335).
    - En el separador **Plugins**, establezca la selección **Lanzar con en solo plugins seleccionados**. Expanda **Espacio de trabajo** y asegúrese de que el plugin que ha creado esté seleccionado y, a continuación, deseccione estos plugins bajo **Plataforma de destino**:
      - `com.ouncelabs.plugin.base`
      - `com.ouncelabs.plugin.base`
      - `com.ouncelabs.plugin.base.nl`
      - `com.ouncelabs.plugin.base.nl`
      - `com.ouncelabs.plugin.enhanced`
      - `com.ouncelabs.plugin.enhanced`
      - `com.ouncelabs.plugin.enhanced.nl`
      - `com.ouncelabs.plugin.enhanced.nl`
  - c. Antes de pulsar **Ejecutar** en el recuadro de diálogo Ejecutar configuraciones, vaya a su directorio de instalación de AppScan Source y ejecute `bin\OunceScanner.exe`.
  - d. Vuelva al recuadro de diálogo Ejecutar configuraciones y pulse **Ejecutar** para iniciar AppScan Source for Analysis y probar el plugin.
8. Habilite el plugin para AppScan Source for Analysis realizando estos pasos:
  - a. Pulse el proyecto con el botón derecho y seleccione **Exportar**.
  - b. En la página Seleccionar del asistente de exportación, expanda **Desarrollo de plugins**, seleccione **Plugins y fragmentos desplegables** y, a continuación, pulse **Siguiente**.
  - c. En la página Plugins y fragmentos desplegables:
    - Vaya al separador **Destino** y establezca el **Directorio** examinando un directorio temporal de su máquina.
    - Vaya al separador **Opciones** y seleccione **Empaquetar plugins como archivos JAR individuales** y **Sustitución de calificadores**.
    - Pulse **Finalizar**.
  - d. Localice el directorio temporal que se ha utilizado como el destino de la exportación para el plugin y, a continuación, abra su carpeta `plugins\`. En esta carpeta, localice el archivo `.jar` que se ha creado y cópielo en `<dir_instalación>\dropins` (donde `<dir_instalación>` es la ubicación de la instalación de AppScan Source).

**Nota:**

- Si no existe el directorio `\dropins`, deberá crearlo manualmente.

- Es posible que si se modifica el directorio de instalación de AppScan Source se necesiten privilegios de administrador.
- e. Localice <dir\_instalación>\configuration\org.eclipse.equinox.simpleconfigurator\bundles.info. Realice una copia de seguridad de este archivo y, a continuación, edite el archivo y añada lo siguiente al final del mismo:
 

```
<mi_plugin>,<versión_mi_plugin>,  
dropins/<mi_plugin>_<versión_mi_plugin>.jar,4,false
```

 Donde:
    - <mi\_plugin> es el nombre del plugin que ha creado.
    - <versión\_mi\_plugin> es el número de versión del plugin que ha creado.

**Nota:** Al inicio de esta entrada, <mi\_plugin>, <versión\_mi\_plugin> y la ubicación dropins/ están separados por comas (,).
  - f. Inicie AppScan Source for Analysis.
  - g. Seleccione **Ayuda > Acerca de AppScan Source for Analysis** en el menú principal y, a continuación, pulse **Detalles de la instalación**. Seleccione el separador **Plugins** y asegúrese de que el plugin figura en la lista.
  - h. Cierre el recuadro de diálogo Detalles de la instalación y comience a utilizar la infraestructura de importación del servidor de aplicaciones.





---

## Capítulo 12. Ejemplo de AppScan Source for Analysis

AppScan Source for Analysis incluye aplicaciones de ejemplo para familiarizarse con el producto.

Después de que AppScan Source for Analysis esté instalado, las aplicaciones de ejemplo se encuentran en <data\_dir>\samples (donde <data\_dir> es la ubicación de los datos de programa AppScan Source, como se describe en “Instalación y ubicaciones de archivo de datos de usuario” en la página 335).

### **Aplicación Java de ejemplo : simpleIOT**

La aplicación de ejemplo simpleIOT es una pequeña aplicación Java que contiene varias vulnerabilidades de seguridad. Puede importarla de forma manual en el entorno de trabajo de AppScan Source for Analysis, o bien, puede importar el archivo de aplicación (SimpleIOT.paf) o el archivo de proyecto (SimpleIOT.ppf) que se incluyen con el ejemplo. Para obtener información acerca de cómo añadir aplicaciones y proyectos, consulte Capítulo 2, “Configuración de aplicaciones y proyectos”, en la página 33.

Una vez que haya añadido el ejemplo a AppScan Source, podrá escanearlo y explorar los resultados.

### **Aplicación de ejemplo para aprender el manejo de la API para Framework for Frameworks: F4FEjbExample.zip**

Este archivador de proyecto de ejemplo se utiliza para demostrar el manejo de la API de Framework for Frameworks. Consulte el manual *IBM Security AppScan Source Utilities Guía del usuario* para obtener más información.



---

## Capítulo 13. El entorno de trabajo de AppScan Source for Analysis

Para obtener el máximo rendimiento del sistema AppScan Source, es preciso que comprenda los conceptos básicos relacionados con el entorno de trabajo de AppScan Source for Analysis y sepa cómo utilizar las opciones que mejor se ajusten a su flujo de trabajo.

---

### El espacio de trabajo de AppScan Source for Analysis

El entorno de trabajo AppScan Source for Analysis se muestra en el *entorno de trabajo*, que consta de perspectivas, vistas y editores que se muestran o están ocultos, en función del contexto.

#### Perspectivas

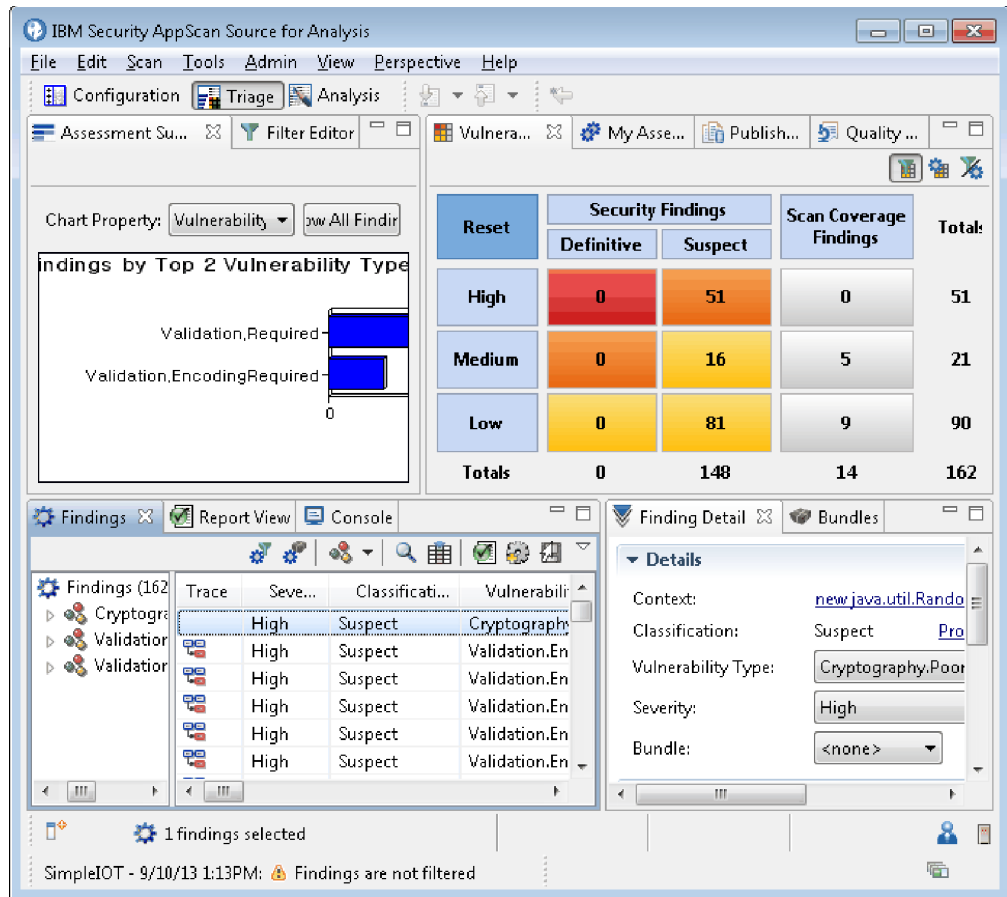
Las tres perspectivas del producto: Configuración, Selección y Análisis, constan de varias vistas. Aunque cada perspectiva se abre con vistas predeterminadas, puede reorganizar las vistas para personalizar cada perspectiva. Las vistas se describen en detalle en la sección Capítulo 14, “Vistas”, en la página 289 de la ayuda.

- Perspectiva Configuración: crear y gestionar aplicaciones, proyectos y atributos.
- Perspectiva Selección: ver los resultados del escaneo para darle prioridad al flujo de trabajo de remediación y separar las vulnerabilidades reales de las potenciales. Esta perspectiva se puede utilizar para aislar los problemas que debe solucionar primero.
- Perspectiva Análisis: profundizar en resultados individuales- revisar el código fuente, consejo de remediación e información de rastreo de AppScan Source.

#### Ventana de espacio de trabajo

La ventana de entorno de trabajo de AppScan Source for Analysis consta de tres elementos:

- Menú principal: menús que permiten acceder a las funciones de AppScan Source for Analysis
- Barra de herramientas: iconos y botones correspondientes a funciones que se utilizan con frecuencia
- Perspectivas: colecciones de vistas
- Vistas: presentaciones y formas de navegar por la información del espacio de trabajo



## Barras de herramientas e información en la parte inferior del espacio de trabajo

- Barra de herramientas de **Vista rápida**: las vistas rápidas son vistas ocultas que se pueden abrir y cerrar con rapidez. Son similares a otras vistas con la diferencia de que no ocupan espacio en la ventana del espacio de trabajo. Las vistas rápidas se representan con botones en la barra de vista rápida, que es la barra de herramientas en la parte inferior izquierda de la ventana del espacio de trabajo. Cuando pulsa el botón de la barra de herramientas de una vista rápida, dicha vista se abre de forma temporal en la perspectiva actual (cubriéndola). Tan pronto como pulse fuera de dicha vista o cuando la vista pierda el foco, se ocultará de nuevo. Para establecer una vista como vista rápida, pulse **Mostrar vista como vista rápida** y luego seleccione la vista en el menú.
- Resultados seleccionados: cuando se seleccionan resultados, un indicador en la parte inferior del espacio de trabajo muestra el número de resultados seleccionados.
- Información de archivo fuente: cuando se abre un archivo fuente, se visualiza en la parte inferior del espacio de trabajo la siguiente información sobre el archivo:
  - Si el archivo es grabable o de sólo lectura. Si intenta editar un archivo de sólo lectura, una solicitud en AppScan Source for Analysis le permitirá establecer el archivo como grabable.
  - Si la modalidad de entrada del sistema operativo es de inserción o sobrescritura.
  - La ubicación de cursor actual en el archivo (número de línea y columna).

- Información de conexión de servidor: al pasar el ratón sobre el icono de usuario se indica que el usuario actualmente ha iniciado una sesión en AppScan Enterprise Server y al pasar el cursor sobre el icono del servidor podrá ver la instancia de AppScan Enterprise Server a la que AppScan Source for Analysis está conectada.
- Cuando se abre el asesoramiento, la parte inferior del espacio de trabajo incluye esta información:
  - Nombre del asesoramiento, y la hora y fecha de su creación.
  - Indicador que permite determinar con rapidez cómo se han aplicado los filtros a los resultados en el asesoramiento. Consulte el apartado “Determinación de filtros aplicados” en la página 168 para obtener más información.
- También se visualiza un indicador de progreso en la parte inferior del espacio de trabajo que indica las acciones en curso. Por ejemplo, este indicador aparece durante los escaneos y en la publicación de asesoramientos. Además, esta sección indica cuando está abierto un asesoramiento.

## Menú principal

La barra de menú principal contiene menús que permiten realizar distintas acciones. Los privilegios de usuario regulan los mandatos disponibles en estos menús.

- “Menú Archivo”
- “Menú Editar” en la página 281
- “Menú Escanear” en la página 282
- “Menú Herramientas” en la página 283
- “Menú Administración” en la página 284
- “Menú Vista” en la página 284
- “Menú Perspectiva” en la página 284
- “Menú Ayuda” en la página 285

## Menú Archivo

El menú **Archivo** ofrece opciones para aplicaciones, proyectos y asesoramientos y le permite salir del producto. Algunos elementos del menú **Archivo** dependen del contexto, en función de la vista activa y del elemento seleccionado en dicha vista.

Tabla 23. Menú Archivo

| Elemento del menú                                            | Descripción                                                                                                                                                                                                              | Acceso directo desde el teclado |
|--------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| <b>Añadir aplicación &gt; Crear una nueva aplicación</b>     | Añadir una nueva aplicación al conjunto de aplicaciones. Esta acción inicia el Asistente para aplicaciones nuevas.                                                                                                       | Control+N                       |
| <b>Añadir aplicación &gt; Abrir una aplicación existente</b> | Inicia un cuadro de diálogo Abrir, que permite examinar y buscar un y añadir una aplicación existente al conjunto de aplicaciones. Los tipos de archivos o directorios que se pueden añadir son .paf, .sln, .dsw y .ewf. | Ctrl+O                          |

Tabla 23. Menú Archivo (continuación)

| Elemento del menú                                                                        | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Acceso directo desde el teclado |
|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| <b>Añadir aplicación &gt; Importar un espacio de trabajo basado en Eclipse existente</b> | Inicia el cuadro de diálogo Añadir espacio de trabajo, que permite añadir un espacio de trabajo Eclipse o IBM Rational Application Developer for WebSphere Software (RAD) existente que contiene proyectos Java. Una vez importado el espacio de trabajo, podrá escanear los proyectos Java que contiene.<br><b>Nota:</b> Antes de importar un espacio de trabajo, asegúrese de haber instalado y actualizado el entorno de desarrollo tal como se describe en “Configuración del entorno de desarrollo para proyectos de Eclipse y Rational Application Developer for WebSphere Software (RAD)” en la página 47. |                                 |
| <b>Añadir aplicación &gt; Importar desde un servidor de aplicaciones</b>                 | Importar una aplicación Java existente desde un servidor de aplicaciones Apache Tomcat o WebSphere Application Server Liberty.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                 |
| <b>Añadir aplicación &gt; Varias aplicaciones</b>                                        | Añadir varias aplicaciones al conjunto de aplicaciones. Esta acción inicia el cuadro de diálogo que le permite especificar un directorio en el que buscar aplicaciones. En estos resultados, puede seleccionar una o varias aplicaciones que añadir.                                                                                                                                                                                                                                                                                                                                                              |                                 |
| <b>Añadir aplicación &gt; Descubrir aplicaciones</b>                                     | Esto inicia Application Discovery Assistant, que permite crear y configurar aplicaciones y proyectos con rapidez para código fuente Java y Microsoft Visual Studio                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                 |
| <b>Eliminar aplicación</b>                                                               | Si una aplicación está en la vista Explorador, esta acción está disponible y al seleccionarla se eliminan las aplicaciones seleccionadas.                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                 |

Tabla 23. Menú Archivo (continuación)

| Elemento del menú                              | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Acceso directo desde el teclado |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| <b>Añadir proyecto &gt; Nuevo proyecto</b>     | Si una aplicación está en la vista Explorador, esta acción está disponible y al seleccionarla le permite añadir un nuevo proyecto a la aplicación. Esta acción inicia el Asistente de proyecto nuevo.                                                                                                                                                                                                                                                                                                                                      |                                 |
| <b>Añadir proyecto &gt; Proyecto existente</b> | Si una aplicación está en la vista Explorador, esta acción está disponible y al seleccionarla le permite añadir un proyecto existente en la aplicación. Esta acción inicia un cuadro de diálogo que permite buscar archivos .ppf, .vcproj, .vcxproj, .csproj, .vbproj, .dsp, o .epf para abrirlos.                                                                                                                                                                                                                                         |                                 |
| <b>Añadir proyecto &gt; Copiar proyecto</b>    | Si se selecciona un proyecto en la vista Explorador, esta acción está disponible y al seleccionarla abre un cuadro de diálogo que le permite copiar el proyecto a otra aplicación o crear una copia del proyecto en la aplicación que actualmente contenga el proyecto.                                                                                                                                                                                                                                                                    |                                 |
| <b>Añadir proyecto &gt; Varios proyectos</b>   | <p>Añadir varios proyectos a la aplicación que está seleccionada en la vista Explorador. Esta acción muestra un recuadro de diálogo que le permite completar una de estas tareas:</p> <ul style="list-style-type: none"> <li>• Especificar un directorio en el que buscar proyectos.</li> <li>• Especificar un espacio de trabajo en el que buscar proyectos.</li> <li>• Especificar un archivo Microsoft Solution en el que buscar proyectos.</li> </ul> <p>En estos resultados, puede seleccionar una o varios proyectos que añadir.</p> |                                 |

Tabla 23. Menú Archivo (continuación)

| Elemento del menú                                           | Descripción                                                                                                                                                                                                                                                                                                                                                     | Acceso directo desde el teclado |
|-------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| <b>Registrar</b>                                            | Registrar la aplicación o proyecto seleccionado con AppScan Source. Debe registrar aplicaciones y proyectos primero para que se puedan publicar en la base de datos de AppScan Source.                                                                                                                                                                          |                                 |
| <b>Anular registro</b>                                      | Anular el registro de la aplicación o proyecto seleccionado.                                                                                                                                                                                                                                                                                                    |                                 |
| <b>Abrir asesoramiento</b>                                  | Inicia un cuadro de diálogo Abrir, que permite examinar y buscar un archivo de asesoramiento de AppScan Source. Los tipos de archivo que se pueden abrir son .ozasmt y .xml.                                                                                                                                                                                    | F7                              |
| <b>Cerrar asesoramiento</b>                                 | Cerrar el asesoramiento que está abierto actualmente en la perspectiva Selección.                                                                                                                                                                                                                                                                               |                                 |
| <b>Guardar asesoramiento</b>                                | Guardar el asesoramiento abierto en un archivo.                                                                                                                                                                                                                                                                                                                 | Control+Mayús+S                 |
| <b>Guardar asesoramiento como</b>                           | Guardar el asesoramiento con otro nombre, guardarlo en otra vía de acceso o ambos.                                                                                                                                                                                                                                                                              |                                 |
| <b>Publicar asesoramiento en AppScan Source</b>             | Almacenar el asesoramiento actual en la base de datos de AppScan Source. La aplicación que se escaneó (o el proyecto o el archivo que contiene la aplicación) deben registrarse primero para que pueda completarse la acción de publicación. Si la aplicación no se ha registrado, se le solicitará que la registre cuando seleccione la acción de publicación. |                                 |
| <b>Publicar asesoramiento en AppScan Enterprise Console</b> | Si AppScan Enterprise Server se ha instalado con la opción Enterprise Console, podrá publicar asesoramientos en ella.<br><br>La página de preferencias de AppScan Enterprise Console debe completarse primero con valores válidos para poder publicar asesoramientos en Enterprise Console.                                                                     |                                 |



Tabla 23. Menú Archivo (continuación)

| Elemento del menú | Descripción                                                                                                                                                                                                                                                                                                                                                                                                | Acceso directo desde el teclado |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| <b>Guardar</b>    | <p>Esta acción está disponible en estas circunstancias:</p> <ul style="list-style-type: none"> <li>Las propiedades de una aplicación se han modificado en la vista Propiedades.</li> <li>Las propiedades de un proyecto se han modificado en la vista Propiedades.</li> <li>Un archivo abierto en el editor interno se ha modificado.</li> </ul> <p>Seleccione esta acción para guardar estos cambios.</p> | Control+S                       |
| <b>Salir</b>      | Salir de AppScan Source for Analysis.                                                                                                                                                                                                                                                                                                                                                                      |                                 |

**Nota:** Para conocer a qué versiones de archivos importados da soporte AppScan Source for Analysis, AppScan Source for Automation y la AppScan Source, consulte <http://www.ibm.com/support/docview.wss?uid=swg27027486>. En esta página, seleccione el separador de la versión de AppScan Source que está utilizando y, a continuación, seleccione el componente de AppScan Source que está utilizando. Si AppScan Source da soporte a la apertura y escando de archivos desde otros entornos de desarrollo, este soporte se muestra en la sección **Compiladores y lenguajes** del separador **Software soportado**.

## Menú Editar

Este menú ofrece una modificación estándar y controles de búsqueda/sustitución. Este menú también se utiliza para mostrar preferencias del producto. Algunos elementos del menú **Editar** dependen del contexto, en función de la vista activa y del elemento seleccionado en dicha vista.

Tabla 24. Menú Editar

| Elemento del menú | Descripción                                                                                                                                              | Acceso directo desde el teclado |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| <b>Cortar</b>     | Copiar y eliminar el texto seleccionado. Utilice esta acción para el texto que está seleccionado en la consola, editor o en varios campos de texto.      | Control+X                       |
| <b>Copiar</b>     | Copiar el texto seleccionado al portapapeles. Utilice esta acción para el texto que está seleccionado en la consola, editor o en varios campos de texto. | Control+C                       |

Tabla 24. Menú Editar (continuación)

| Elemento del menú       | Descripción                                                                                                                                                                   | Acceso directo desde el teclado |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| <b>Pegar</b>            | Pegar texto que se ha copiado o cortado. Esta acción se suele utilizar para información de duplicación y para reproducirla en otra parte del producto.                        | Control+V                       |
| <b>Renombrar</b>        | Cambiar el nombre del objeto seleccionado. Los objetos de los que se puede cambiar el nombre son aplicaciones, proyectos, asesoramientos y paquetes.                          | F2                              |
| <b>Eliminar</b>         | Eliminar el objeto seleccionado.                                                                                                                                              | Suprimir                        |
| <b>Seleccionar todo</b> | Seleccione todo el cuerpo del texto. Utilice esta acción para el texto en la consola, editor o en varios campos de texto.                                                     | Control+A                       |
| <b>Renovar</b>          | Renuevo el contenido de la aplicación, proyecto o vista seleccionada.                                                                                                         | F5                              |
| <b>Buscar</b>           | Busque texto en la consola, editor o busque resultados en la tabla de resultados.                                                                                             | Control+F                       |
| <b>Buscar siguiente</b> | Si la acción de búsqueda se ha utilizado para buscar texto en la consola o el editor, utilice esta acción para encontrar la siguiente instancia del texto.                    | F3                              |
| <b>Preferencias</b>     | Seleccione esto para abrir el cuadro de diálogo Preferencias. Las preferencias son seleccione personales sobre el aspecto y el funcionamiento de AppScan Source for Analysis. |                                 |

## Menú Escanear

En el menú **Escanear**, puede gestionar escaneos de una aplicación, proyecto o archivo seleccionado.

Tabla 25. Menú Escanear

| Elemento del menú    | Descripción                                                                                             | Acceso directo desde el teclado |
|----------------------|---------------------------------------------------------------------------------------------------------|---------------------------------|
| <b>Escanear todo</b> | Escanea todas las aplicaciones. El escaneo se ejecutará con la configuración de escaneo predeterminada. |                                 |

Tabla 25. Menú Escanear (continuación)

| Elemento del menú             | Descripción                                                                                                                                                                                                                                                                                                                 | Acceso directo desde el teclado |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| <b>Escanear selección</b>     | Escanear la aplicación proyecto o archivo seleccionados. El escaneo se ejecutará con la configuración de escaneo predeterminada.                                                                                                                                                                                            | F4                              |
| <b>Escanear de nuevo</b>      | Volver a escanear destinos de asesoramiento. La última configuración de escaneo que se ha utilizado para escanear el elemento (o los elementos seleccionados) se utilizará de nuevo para el escaneo.                                                                                                                        |                                 |
| <b>Cancelar escaneo</b>       | Termina el escaneo y no genera ningún resultado.                                                                                                                                                                                                                                                                            |                                 |
| <b>Detener escaneo</b>        | Detiene el escaneo y genera resultados parciales.                                                                                                                                                                                                                                                                           |                                 |
| <b>Compilar configuración</b> | La configuración define los parámetros de creación del proyecto, como definiciones de preprocesador o vías de acceso de inclusión. Generalmente aparece una configuración llamada <b>Release</b> o <b>Debug</b> procedente de un proyecto importado.<br><br>Este elemento de menú está inhabilitado cuando no es aplicable. |                                 |

## Menú Herramientas

Este menú incluye opciones para comparar asesoramientos y generar informes y para revisar archivos o resultados en un editor. Algunos elementos del menú **Herramientas** dependen del contexto, en función de la vista activa y del elemento seleccionado en dicha vista.

Tabla 26. Menú Herramientas

| Elemento del menú                      | Descripción                                                                                                                                                                                                                                                   |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Diferencia entre asesoramientos</b> | Esta acción abre un cuadro de diálogo que permite seleccionar dos asesoramientos que se deben comparar.                                                                                                                                                       |
| <b>Generar informe de resultados</b>   | Generar un informe de los resultados o contenido de paquetes seleccionados. Se debe seleccionar una vista de resultados o paquetes al emitir esta acción. Si no se seleccionan resultados en la vista, el informe contendrá todos los resultados de la vista. |
| <b>Generar informe</b>                 | Generar un informe que le permita ver todos resultados en función de determinados requisitos o directrices de conformidad.                                                                                                                                    |

Tabla 26. Menú Herramientas (continuación)

| Elemento del menú              | Descripción                                                                                                                                                                                          |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Abrir en editor interno</b> | Abrir un archivo en el editor AppScan Source for Analysis interno. Esta acción puede utilizarse para un resultado seleccionado y hará que el archivo asociado con el resultado se abra en el editor. |
| <b>Abrir en editor externo</b> | Abrir un archivo utilizando un editor externo. Esta acción puede utilizarse para un resultado seleccionado y hará que el archivo asociado con el resultado se abra en el editor.                     |

## Menú Administración

El menú **Administración** proporciona acciones que le permiten gestionar usuarios y mostrar información de auditoría.

Tabla 27. Menú Administración

| Elemento del menú         | Descripción                                                                                                                                                                             |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Gestionar usuarios</b> | Esta acción muestra un cuadro de diálogo que le permite crear y editar usuarios y permisos.<br><br>Debe tener permisos administrativos de AppScan Source para poder gestionar usuarios. |
| <b>Auditoría</b>          | Esta acción muestra una vista que le permite ver información de auditoría, como sucesos de autenticación.                                                                               |

Consulte la publicación *IBM Security AppScan Source Guía de instalación y administración* para obtener información detallada acerca de las tareas administrativas.

## Menú Vista

El menú **Vista** controla la visualización de cada vista o selecciona una vista abierta.

Para obtener más información acerca de las vistas disponibles en AppScan Source for Analysis, consulte AppScan Source for Analysis Vistas.

## Menú Perspectiva

El menú **Perspectiva** controla la visualización de las *perspectivas* de AppScan Source for Analysis que son conjuntos preconfiguradas de vistas y opciones.

Tabla 28. Menú Perspectiva

| Elemento del menú    | Descripción                                                                     | Acceso directo desde el teclado |
|----------------------|---------------------------------------------------------------------------------|---------------------------------|
| <b>Configuración</b> | Esta perspectiva permite crear y gestionar aplicaciones, proyectos y atributos. | Alt+1                           |

Tabla 28. Menú Perspectiva (continuación)

| Elemento del menú              | Descripción                                                                                                                                                                                                                                                     | Acceso directo desde el teclado |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| <b>Selección</b>               | Esta perspectiva permite ver resultados del escaneo para darle prioridad al flujo de trabajo de remediación y separar las vulnerabilidades reales de las potenciales. Esta perspectiva se puede utilizar para aislar los problemas que debe solucionar primero. | Alt+2                           |
| <b>Análisis</b>                | La perspectiva le permite profundizar en resultados individuales y revisar el código fuente, consejo de remediación e información de rastreo de AppScan Source.                                                                                                 | Alt+3                           |
| <b>Restablecer perspectiva</b> | Al seleccionar esto, la perspectiva actualmente mostrada vuelve a sus valores y diseño predeterminados.                                                                                                                                                         |                                 |

## Menú Ayuda

El menú **Ayuda** incluye acciones que abren diversas herramientas que ayudan con el uso del producto. Estas incluyen la bienvenida al producto, asistencia al usuario en línea y la Base de datos de conocimientos de AppScan Source Security.

Tabla 29. Menú Ayuda

| Elemento del menú                                | Descripción                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Bienvenido</b>                                | Al seleccionar esto, se abre la vista Bienvenido de AppScan Source for Analysis. Esta vista de bienvenida ofrece enlaces rápidos a diversos recursos de ayuda, incluida información sobre un canal de información RSS de X-Force.                                                                        |
| <b>Contenido de la Ayuda</b>                     | Al seleccionar esto, se abre la asistencia al usuario del producto AppScan Source for Analysis.                                                                                                                                                                                                          |
| <b>Base de datos de conocimiento de Security</b> | Esta acción hace que se abra la Base de datos de conocimientos de AppScan Source Security. La base de datos de conocimientos proporciona inteligencia para cada vulnerabilidad, ofreciendo descripciones precisas acerca de la causa raíz, la gravedad de riesgo y los consejos de solución procesables. |
| <b>Registros</b>                                 | Al seleccionar esto, se abre la vista Registros. En la vista, los separadores le permiten seleccionar el archivo de registro que se mostrará.                                                                                                                                                            |

Tabla 29. Menú Ayuda (continuación)

| Elemento del menú                             | Descripción                                                                                                                         |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| AboutIBM Security AppScan Source for Analysis | Al seleccionarlo, se abre un cuadro de diálogo que proporciona información sobre el producto acerca de AppScan Source for Analysis. |

## Barras de herramientas

Las barras de herramientas del entorno de trabajo de AppScan Source for Analysis proporcionan accesos directos gráficos a mandatos. Para identificar un icono de barra de herramientas determinado, coloque el cursor del ratón sobre el icono hasta que aparezca la ayuda flotante. Los botones de la barra de herramientas representan operaciones que se utilizan con frecuencia (también están en el menú **Principal**). Las operaciones de la barra de herramientas dependen del contexto.

La barra de herramientas principal proporciona enlaces rápidos a perspectivas de AppScan Source for Analysis. Además, la mayoría de las vistas tienen barras de herramientas que ofrecen una forma rápida de inicio de acciones comunes relacionadas con la vista.

## Ayuda flotante

La ayuda contextual es una forma de ayuda según contexto que se visualiza en una pequeña ventana cuando el puntero de ratón está situado sobre un elemento de la interfaz. En la ventana emergente aparece una breve descripción del elemento de la interfaz.

Además de proporcionar ayuda contextual para botones e iconos, AppScan Source for Analysis ofrece ayuda contextual en diferentes lugares, como:

- En la vista Explorador, la ayuda contextual está disponible para indicar el nombre del archivo y vía de acceso de aplicaciones, proyectos y archivos. La ayuda contextual también indica si una aplicación o proyecto están registrados.
- En la vista de rastreo, al mover el cursor sobre los nodos de rastreo en el gráfico, se proporciona información sobre el nodo.
- En la sección **Rastreo** de vista Editor de filtros, al mover el cursor sobre una entrada de rastreo, se proporcionan detalles acerca de la entrada.
- En sección **Valores avanzados** de la vista Configuración del escaneo, la ayuda contextual está disponible para cada valor.
- Si mueve el cursor sobre una barra de gráfico en la vista Resumen de asesoramiento proporciona el número exacto de resultados representados por la barra.
- En la barra de estado de entorno de trabajo (situada en la parte inferior del entorno de trabajo), si mueve el cursor sobre el icono de usuario, se muestra la ayuda contextual que identifica el usuario que ha iniciado la sesión. Si mueve el cursor sobre el icono de servidor se inicia la ayuda contextual que indica a Enterprise Server que AppScan Source for Analysis está conectado.

## Barra de estado

La barra de estado, situada en la parte inferior del espacio de trabajo, muestra mensajes informativos que identifican la acción, como por ejemplo un escaneo.

Por ejemplo, durante un escaneo, la barra de estado puede mostrar Escaneando <Nombre proyecto> con un indicador de progreso. Además, la etapa actual del escaneo se muestra, por ejemplo, Preparando análisis de vulnerabilidad: 99%. Cuando se completa el escaneo, el tiempo transcurrido se muestra en la barra de estado.

La barra de estado también incluye información acerca de la conexión entre usuario y servidor. Si mueve el cursor sobre el icono de usuario, se muestra la ayuda contextual que identifica el usuario que ha iniciado la sesión. Si mueve el cursor sobre el icono de servidor se inicia la ayuda contextual que indica a Enterprise Server que AppScan Source for Analysis está conectado.





---

## Capítulo 14. Vistas

El entorno de trabajo de AppScan Source for Analysis consta de varias perspectivas y vistas, que contienen diversos datos de asesoramiento o de escaneo.

Las vistas de AppScan Source for Analysis ofrecen presentaciones alternativas de resultados (algunas de las cuales dan soporte a la edición de código) y le permiten navegar por la información del espacio de trabajo. Por ejemplo, la vista Explorador muestra aplicaciones, proyectos y otros recursos. Una vista puede mostrarse sola o junto a otras vistas en un cuaderno con separadores. Puede cambiar el diseño de una perspectiva abriendo y cerrando vistas y colocándolas en diferentes posiciones en la ventana del entorno de trabajo.

Las vistas se describen en más detalle en estas secciones:

- “Vistas de configuración”
- “Vistas que ayudan con la salida de escaneo” en la página 312
- “Vistas que ayudan con la selección” en la página 315
- “Vistas que permiten investigar un resultado único” en la página 326
- “Vistas que permiten trabajar con asesoramientos” en la página 331
- “Vista Paquetes” en la página 334

---

### Vistas de configuración

Las vistas en esta sección se utilizan para configurar AppScan Source.

- “Vista Reglas personalizadas”
- “Vista Explorador” en la página 85
- “Vista Biblioteca de reglas de patrón” en la página 295
- “Vista Propiedades” en la página 296
- “Vista Configuración del escaneo” en la página 119
- “Editor de informe” en la página 231

### Vista Reglas personalizadas

En la vista Reglas personalizadas se crean reglas personalizadas con el Asistente de reglas personalizadas. Puede añadir, ver o suprimir reglas existentes.

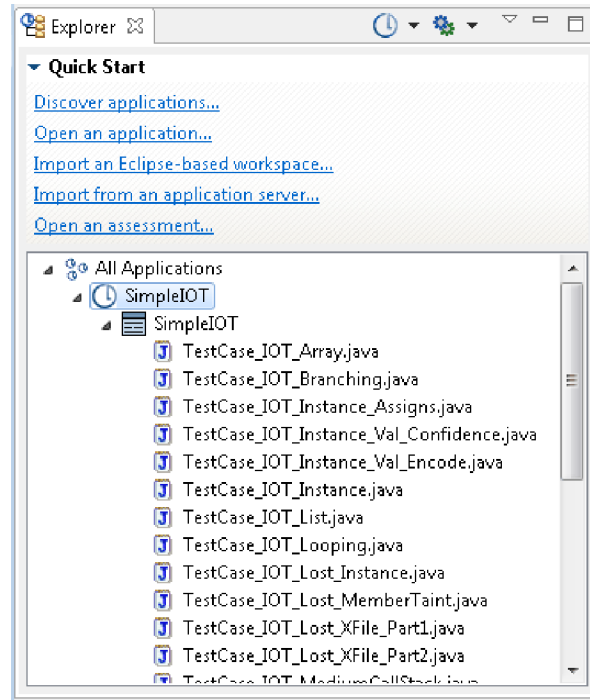
Consulte “Creación de reglas personalizadas” en la página 240 para obtener más información.

### Vista Explorador

La vista Explorador contiene una sección **Inicio rápido** en la parte superior y una sección Explorador en la parte inferior que contiene un nodo, **Todas las aplicaciones**. La sección **Inicio rápido** sección contiene varios enlaces útiles que inician acciones comunes. La sección Explorador está formada por un panel de árbol que ofrece una vista jerárquica de los recursos: aplicaciones, proyectos, directorios y archivos de proyecto, con **Todas las aplicaciones** como raíz. Puede navegar por estos recursos como si estuviera en un navegador de archivos. A medida que navega por la vista, el estado de selección del árbol determina los separadores disponibles en la vista Propiedades.

- “Información general” en la página 86
- “Sección Inicio rápido” en la página 86
- “Botones de la barra de herramientas” en la página 87
- “Opciones del menú del botón derecho ” en la página 88
- “Indicadores de aplicaciones y proyectos ” en la página 90

## Información general



En la vista Explorador, puede añadir aplicaciones y proyectos, y escanear código utilizando los botones de la barra de herramienta, los enlaces en la sección **Inicio rápido** o los mandatos del menú que aparecen al pulsar con el botón derecho en la sección Explorador. Una vez añadidas las aplicaciones, la sección Explorador ofrece indicadores visuales de las aplicaciones y proyectos y del estado de cada uno de ellos.

**Consejo:** En la vista Explorador, la ayuda contextual está disponible para indicar el nombre del archivo y vía de acceso de aplicaciones, proyectos y archivos. La ayuda contextual también indica si una aplicación o proyecto están registrados.

## Sección Inicio rápido

La sección **Inicio rápido** ofrece estos enlaces para iniciar tareas comunes:

- **Descubrir aplicaciones:** Esto inicia Application Discovery Assistant, que permite crear y configurar aplicaciones y proyectos con rapidez para código fuente Java y Microsoft Visual Studio
- **Abrir una aplicación:** Inicia un cuadro de diálogo Abrir, que permite examinar y buscar un y añadir una aplicación existente al conjunto de aplicaciones. Los tipos de archivos o directorios que se pueden añadir son .paf, .sln, .dsw y .ewf.
- **Importar un espacio de trabajo basado en Eclipse:** Inicia el cuadro de diálogo Añadir espacio de trabajo, que permite añadir un espacio de trabajo Eclipse o

IBM Rational Application Developer for WebSphere Software (RAD) existente que contiene proyectos Java. Una vez importado el espacio de trabajo, podrá escanear los proyectos Java que contiene.

**Nota:** Antes de importar un espacio de trabajo, asegúrese de haber instalado y actualizado el entorno de desarrollo tal como se describe en “Configuración del entorno de desarrollo para proyectos de Eclipse y Rational Application Developer for WebSphere Software (RAD)” en la página 47.

- **Importar desde un servidor de aplicaciones:** Importar una aplicación Java existente desde un servidor de aplicaciones Apache Tomcat o WebSphere Application Server Liberty.
- **Abrir un asesoramiento:** Inicia un cuadro de diálogo Abrir, que permite examinar y buscar un archivo de asesoramiento de AppScan Source. Los tipos de archivo que se pueden abrir son .ozasmt y .xml.

## Botones de la barra de herramientas

Tabla 30. Botones de la barra de herramientas

| Acción                    | Icono                                                                               | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Añadir menú de aplicación |    | Cuando pulsa la flecha hacia abajo en el botón <b>Añadir menú de aplicación</b> , puede seleccionar acciones para crear una nueva aplicación, abrir una aplicación existente, importar un espacio de trabajo o iniciar Application Discovery Assistant.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Escanear selección        |  | El botón <b>Escanear selección</b> permite escanear el objeto que se ha seleccionado en la sección Explorador. Se utilizará la configuración de escaneo predeterminada para el escaneo. Para elegir otra configuración del escaneo que se utilizará para el escaneo, pulse la flecha hacia abajo en el botón <b>Escanear selección</b> . Seleccione la configuración de escaneo que desee utilizar. O bien, seleccione la acción <b>Editar configuraciones</b> para establecer una configuración de escaneo diferente como valor predeterminado (en la vista Configuración del escaneo, seleccione la configuración que desea establecer como valor predeterminado y, a continuación, pulse <b>Seleccionar como valor predeterminado</b> ). |

Tabla 30. Botones de la barra de herramientas (continuación)

| Acción   | Icono | Descripción                                                                                                          |
|----------|-------|----------------------------------------------------------------------------------------------------------------------|
| Menú Ver |       | El botón <b>Menú Ver</b> abre un menú que permite renovar la sección Explorador y ocultar los elementos registrados. |

## Opciones del menú del botón derecho

La disponibilidad de las opciones del menú que aparece al pulsar el botón derecho del ratón están determinadas por el elemento seleccionado en la sección Explorador.

- Al seleccionar **Todas las aplicaciones** en la sección Explorador, estas opciones del menú que aparece al pulsar el botón derecho del ratón están disponibles:
    - **Escanear todas las aplicaciones:** Escanea todas las aplicaciones. El escaneo se ejecutará con la configuración de escaneo predeterminada.
    - **Escanear todas las aplicaciones con:** Seleccione la configuración de escaneo que desee utilizar. O bien, seleccione la acción **Editar configuraciones** para establecer una configuración de escaneo diferente como valor predeterminado (en la vista Configuración del escaneo, seleccione la configuración que desee establecer como valor predeterminado y, a continuación, pulse **Seleccionar como valor predeterminado**).
    - **Añadir aplicación**
      - **Crear una nueva aplicación:** Añadir una nueva aplicación al conjunto de aplicaciones. Esta acción inicia el Asistente para aplicaciones nuevas.
      - **Abrir una aplicación existente:** Inicia un cuadro de diálogo Abrir, que permite examinar y buscar un y añadir una aplicación existente al conjunto de aplicaciones. Los tipos de archivos o directorios que se pueden añadir son .paf, .sln, .dsw y .ewf.
      - **Importar un espacio de trabajo basado en Eclipse existente:** Inicia el cuadro de diálogo Añadir espacio de trabajo, que permite añadir un espacio de trabajo Eclipse o IBM Rational Application Developer for WebSphere Software (RAD) existente que contiene proyectos Java. Una vez importado el espacio de trabajo, podrá escanear los proyectos Java que contiene.
- Nota:** Antes de importar un espacio de trabajo, asegúrese de haber instalado y actualizado el entorno de desarrollo tal como se describe en “Configuración del entorno de desarrollo para proyectos de Eclipse y Rational Application Developer for WebSphere Software (RAD)” en la página 47.
- **Descubrir aplicaciones:** Esto inicia Application Discovery Assistant, que permite crear y configurar aplicaciones y proyectos con rapidez para código fuente Java y Microsoft Visual Studio
  - **Expandir todo**
  - **Contraer todo**
  - **Propiedades:** al seleccionarla, se abre la vista Propiedades para el elemento seleccionado.
  - Al seleccionar una aplicación en la sección Explorador, estas opciones del menú que aparece al pulsar el botón derecho del ratón están disponibles:

- **Escanear la aplicación:** Escanear la aplicación proyecto o archivo seleccionados. El escaneo se ejecutará con la configuración de escaneo predeterminada.
- **Escanear aplicación con:** Seleccione la configuración de escaneo que desee utilizar. O bien, seleccione la acción **Editar configuraciones** para establecer una configuración de escaneo diferente como valor predeterminado (en la vista Configuración del escaneo, seleccione la configuración que desea establecer como valor predeterminado y, a continuación, pulse **Seleccionar como valor predeterminado**).
- **Añadir proyecto**
  - **Nuevo proyecto:** Si una aplicación está en la vista Explorador, esta acción está disponible y al seleccionarla le permite añadir un nuevo proyecto a la aplicación. Esta acción inicia el Asistente de proyecto nuevo.
  - **Proyecto existente:** Si una aplicación está en la vista Explorador, esta acción está disponible y al seleccionarla le permite añadir un proyecto existente en la aplicación. Esta acción inicia un cuadro de diálogo que permite buscar archivos .ppf, .vcproj, .vcxproj, .csproj, .vbproj, .dsp, o .epf para abrirlos.
  - **Varios proyectos:** Añadir varios proyectos a la aplicación que está seleccionada en la vista Explorador. Esta acción muestra un recuadro de diálogo que le permite completar una de estas tareas:
    - Especificar un directorio en el que buscar proyectos.
    - Especificar un espacio de trabajo en el que buscar proyectos.
    - Especificar un archivo Microsoft Solution en el que buscar proyectos.

En estos resultados, puede seleccionar una o varios proyectos que añadir.
- **Eliminar aplicación:** Si una aplicación está en la vista Explorador, esta acción está disponible y al seleccionarla se eliminan las aplicaciones seleccionadas.
- **Añadir resultado personalizado:** esta acción inicia el cuadro de diálogo Crear resultado personalizado, que le permite crear un resultado personalizado para la aplicación seleccionada.
- **Renovar:** Renuevo el contenido de la aplicación, proyecto o vista seleccionada.
- Registrar/eliminar registro:
  - **Registrar aplicación:** Registrar la aplicación o proyecto seleccionado con AppScan Source. Debe registrar aplicaciones y proyectos primero para que se puedan publicar en la base de datos de AppScan Source.
  - **Registrar aplicación como...:** seleccione esta opción para registrar una aplicación con un nuevo nombre.
  - **Eliminar registro de la aplicación:** Anular el registro de la aplicación o proyecto seleccionado.
  - **Localizar:** seleccione esta opción para asociar una aplicación o proyecto local con uno que haya registrado otro usuario de AppScan Source.
- **Expandir todo**
- **Contraer todo**
- **Propiedades:** al seleccionarla, se abre la vista Propiedades para el elemento seleccionado.
- Al seleccionar un proyecto en la sección Explorador, estas opciones del menú que aparece al pulsar el botón derecho del ratón están disponibles:
  - **Escanear proyecto:** Escanear la aplicación proyecto o archivo seleccionados. El escaneo se ejecutará con la configuración de escaneo predeterminada.

- **Escanear proyecto con:** Seleccione la configuración de escaneo que desee utilizar. O bien, seleccione la acción **Editar configuraciones** para establecer una configuración de escaneo diferente como valor predeterminado (en la vista Configuración del escaneo, seleccione la configuración que desea establecer como valor predeterminado y, a continuación, pulse **Seleccionar como valor predeterminado**).
- **Copiar proyecto:** Si se selecciona un proyecto en la vista Explorador, esta acción está disponible y al seleccionarla abre un cuadro de diálogo que le permite copiar el proyecto a otra aplicación o crear una copia del proyecto en la aplicación que actualmente contenga el proyecto.
- **Eliminar proyecto:** Eliminar el objeto seleccionado.
- Registrar/eliminar registro:
  - **Registrar proyecto:** Registrar la aplicación o proyecto seleccionado con AppScan Source. Debe registrar aplicaciones y proyectos primero para que se puedan publicar en la base de datos de AppScan Source.
  - **Eliminar registro del proyecto:** Anular el registro de la aplicación o proyecto seleccionado.
  - **Localizar:** seleccione esta opción para asociar una aplicación o proyecto local con uno que haya registrado otro usuario de AppScan Source.
- **Expandir todo**
- **Contraer todo**
- **Propiedades:** al seleccionarla, se abre la vista Propiedades para el elemento seleccionado.
- Al seleccionar un archivo en la sección Explorador, estas opciones del menú que aparece al pulsar el botón derecho del ratón están disponibles:
  - **Escanear archivo:** Escanear la aplicación proyecto o archivo seleccionados. El escaneo se ejecutará con la configuración de escaneo predeterminada.
  - **Escanear archivo con:** Seleccione la configuración de escaneo que desee utilizar. O bien, seleccione la acción **Editar configuraciones** para establecer una configuración de escaneo diferente como valor predeterminado (en la vista Configuración del escaneo, seleccione la configuración que desea establecer como valor predeterminado y, a continuación, pulse **Seleccionar como valor predeterminado**).
  - **Excluir de los escaneos:** elimina de los escaneos el archivo seleccionado.
  - **Abrir en editor interno:** abre el archivo seleccionado en el editor de AppScan Source (en la perspectiva Análisis).
  - **Abrir en editor externo:** escoja un editor externo en el que abrir el archivo seleccionado.
  - **Propiedades:** al seleccionarla, se abre la vista Propiedades para el elemento seleccionado.

## Indicadores de aplicaciones y proyectos

Esta tabla identifica los iconos de aplicación y de proyecto de la vista Explorador.

*Tabla 31. Iconos de aplicación y de proyecto*

| Tipo de aplicación o proyecto | No registrado                                                                       | Registrado                                                                          | Falta/No se encuentra                                                                 |
|-------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| Aplicación importada          |  |  |  |

Tabla 31. Iconos de aplicación y de proyecto (continuación)

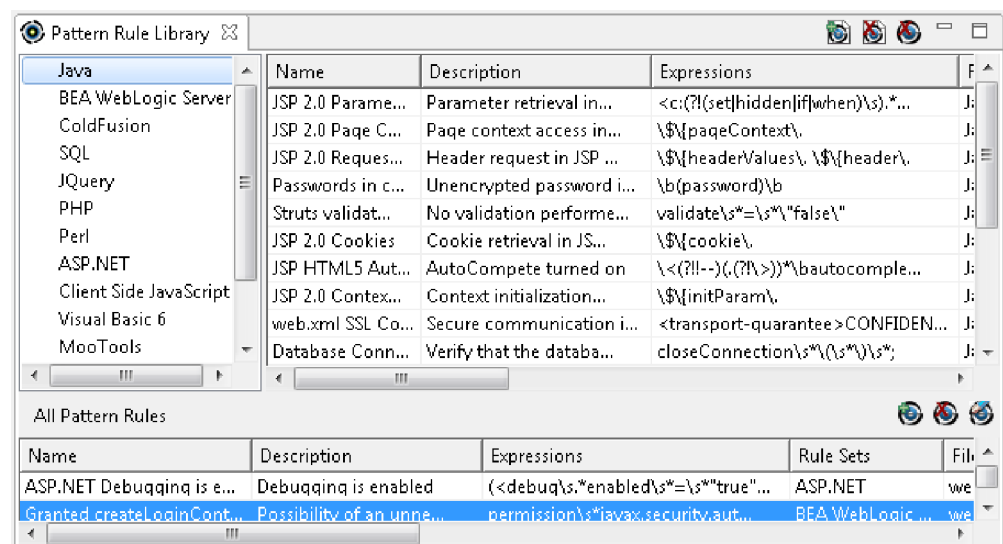
| Tipo de aplicación o proyecto                                                     | No registrado | Registrado | Falta/No se encuentra |
|-----------------------------------------------------------------------------------|---------------|------------|-----------------------|
| Aplicación creada manualmente o creada utilizando Application Discovery Assistant |               |            |                       |
| Proyecto importado                                                                |               |            |                       |
| Proyecto creado manualmente o creado utilizando Application Discovery Assistant   |               |            |                       |

La vista Explorador muestra aplicaciones y proyectos locales, así como aquellos registrados en el servidor (los registrados en el servidor que no se han guardado localmente, por ejemplo, las aplicaciones y los proyectos registrados por otros usuarios, aparecen sombreados). Si pulsa el botón **Menú Ver** de la barra de herramientas y conmuta al elemento de menú **Ocultar elementos registrados en el servidor** para que no esté seleccionado, puede ver las aplicaciones y proyectos del servidor existentes. Si un proyecto aparece sombreado, puede pulsar con el botón derecho y seleccionar **Localizar** en el menú.

## Vista Biblioteca de reglas de patrón

El escaneo basado en patrones es un análisis del código fuente basado en criterios de búsqueda personalizados. La vista Biblioteca de reglas de patrón le permite ver las reglas basadas en patrones existentes, por idioma (incluida la biblioteca de reglas de patrones AppScan Source predeterminada). Además, la vista le permite añadir reglas y patrones para el escaneo basado en patrón.

Después de crear una biblioteca de reglas, puede aplicar el análisis de patrón a aplicaciones o proyectos específicos. Consulte “Personalización con reglas basadas en patrón” en la página 247 para ver detalles sobre las búsquedas de patrón.



## Vista Propiedades

El contenido de la vista Propiedades depende del elemento seleccionado en la vista Explorador. Las propiedades se aplican a todas las aplicaciones, aplicaciones individuales, proyectos o archivos. Las propiedades visibles dependen del idioma o del tipo de proyecto seleccionado.

- “Vista Propiedades: todas las aplicaciones”
- “Vista Propiedades: aplicación seleccionada” en la página 258
- “Vista Propiedades: proyecto seleccionado” en la página 259
- “Propiedades de archivo” en la página 305

### Vista Propiedades: todas las aplicaciones

Si selecciona **Todas las aplicaciones** en la vista Explorador, la vista Propiedades visualiza los separadores Visión general y filtros.

#### Visión general

El separador Visión general muestra atributos globales. Los *atributos* son agrupaciones con nombre de elementos definidos por el usuario con características similares. Puede añadir o suprimir atributos y sus valores.

#### Filtros

Este separador permite especificar filtros existentes para todas las aplicaciones. También permite especificar cómo desea aplicar los filtros (un filtro se puede aplicar de forma directa o de forma inversa). Consulte Capítulo 5, “Selección y análisis”, en la página 145 para obtener información sobre los filtros y “Aplicación de filtros globalmente” en la página 168 para obtener detalles sobre su aplicación global.

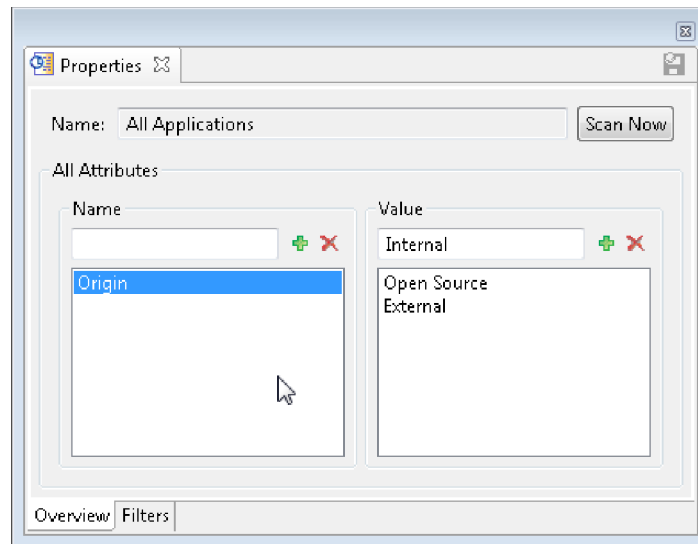
Los resultados filtrados no aparecen en los resultados o factor del escaneo en métricas de la aplicación o del proyecto.

#### Adición y eliminación de atributos globales:

Debe definir atributos para **Todas las aplicaciones** antes de agrupar atributos para aplicaciones.



## Acerca de esta tarea



Si desea suprimir un atributo global o su valor, seleccione el nombre del atributo o el valor del atributo y, a continuación, pulse **Eliminar atributo**. El nombre o valor deja de aparecer en la lista.

**Nota:** El hecho de suprimir un atributo no afecta a los resultados históricos.

Para añadir un atributo global y su valor, siga los pasos que se indican a continuación.

### Procedimiento

1. Seleccione **Todas las aplicaciones**.
2. En la vista Propiedades separador Visión general, escriba un nombre para el atributo.
3. Pulse **Añadir atributo**. El nombre del atributo aparece en la lista Nombre.
4. Seleccione el atributo con nombre.
5. Escriba un **Valor** para el atributo.
6. Pulse **Añadir valor**. El valor del atributo aparece en la lista de valores.

### Vista Propiedades: aplicación seleccionada

En esta vista puede configurar atributos para la aplicación seleccionada. Los atributos de la aplicación dependen de los atributos globales creados con anterioridad.

- “Visión general” en la página 258
- “Exclusiones y filtros” en la página 258
- “Reglas y conjuntos de reglas” en la página 258
- “Resultados modificados” en la página 259
- “Resultados personalizados” en la página 259

### Visión general

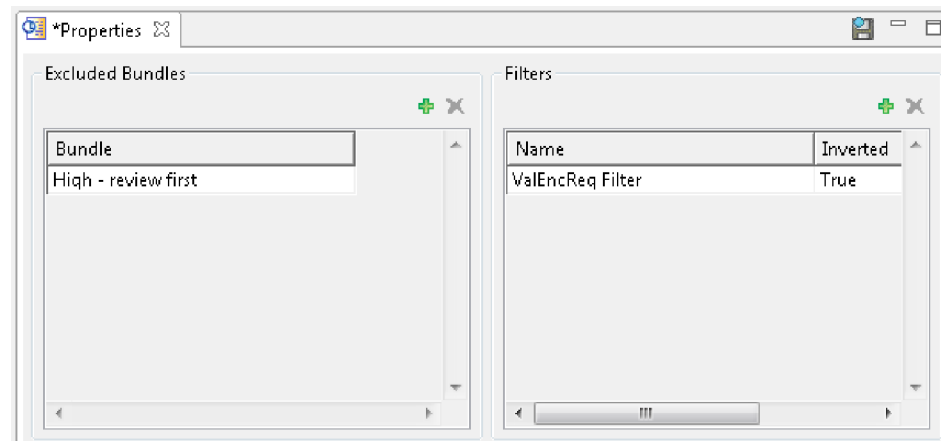
El separador Visión general muestra:

- Nombre de aplicación. La aplicación se puede renombrar especificando un nombre nuevo en el campo.
- Atributos de aplicación

## Exclusiones y filtros

Este separador permite especificar filtros existentes a la aplicación seleccionada, y la forma en que desea aplicar los filtros (un filtro se puede aplicar de forma directa o de forma inversa). En el separador, también puede gestionar los paquetes que excluyen resultados de escaneo. Consulte Capítulo 5, “Selección y análisis”, en la página 145 para obtener información sobre los filtros y “Aplicación de filtros globalmente” en la página 168 para obtener más detalles sobre cómo aplicarlos globalmente.

Los resultados excluidos y filtrados no aparecen en los resultados o factor del escaneo en métricas de la aplicación o del proyecto.



## Reglas y conjuntos de reglas

Cuando selecciona una aplicación en la vista Explorador, el separador Reglas de patrón y conjuntos de reglas de la vista Propiedades le permite añadir reglas de patrón y conjuntos de reglas que se aplicarán al escanear la aplicación. Si utiliza un escaneo basado en patrón, busca patrones de texto que desea que aparezcan como resultados. Las reglas individuales y los conjuntos de reglas se pueden aplicar a las aplicaciones y a los proyectos. Consulte “Personalización con reglas basadas en patrón” en la página 247 para obtener información sobre el análisis basado en patrones y “Aplicación de reglas de patrón y de conjuntos de reglas” en la página 254 para obtener más información sobre cómo aplicar reglas y conjuntos de reglas en la vista Propiedades.

## Resultados modificados

En el separador Resultados modificados puede ver, editar o suprimir cualquier resultado anteriormente modificado o modificar un resultado existente. Los *resultados modificados* son resultados con el tipo de vulnerabilidad, gravedad, clasificación o notas alterados.

## Resultados personalizados

En el separador Resultados personalizados puede ver, añadir, editar o suprimir resultados personalizados. Consulte “Resultados personalizados” en la página 183 para obtener más información.

### Creación de un atributo de aplicación:

#### Procedimiento

1. En el separador Visión general, pulse **Añadir atributos**.
2. En el cuadro de diálogo **Atributos globales**, seleccione el nombre del atributo que desea aplicar a la aplicación.
3. Pulse la columna **Valor** y seleccione el valor del atributo en la lista.

### Vista Propiedades: proyecto seleccionado

En esta modalidad de la vista Propiedades, puede configurar parámetros para el proyecto seleccionado. Los atributos del proyecto dependen de los atributos globales creados previamente. Las propiedades varían en función del proyecto seleccionado.

- “Separador visión general del proyecto seleccionado” en la página 259
- “Filtros” en la página 261
- “Reglas de patrón y Conjuntos de reglas” en la página 261
- “Extensiones de archivo” en la página 261
- “Orígenes” en la página 262
- “Dependencias del proyecto JavaServer Page (JSP)” en la página 263
- “Dependencias del proyecto” en la página 263
- “Compilación” en la página 263
- “Optimizaciones” en la página 264
- “Separador Precompilar (solo ASP.NET)” en la página 264

### Separador visión general del proyecto seleccionado

El separador Visión general muestra:

- **Nombre** del proyecto. El proyecto se puede renombrar especificando un nombre nuevo en el campo.
- Nombre de **archivo** y vía de acceso del proyecto
- **Tipo de proyecto**
- Configuración: Esta sección visualiza la configuración de destino. Para proyectos .NET y C++, esta sección visualiza la configuración de destino que se ha guardado en el separador Dependencias del proyecto. Con todos los otros tipos de proyecto, esta sección visualiza **Predeterminado**.
- Opción de filtro: seleccione **Filtrar resultados contenidos en fuentes externas** para filtrar los resultados descubiertos en archivos que no son archivos de origen del proyecto escaneado. Esta opción reduce el ruido para los proyectos cuando los resultados se notifican en archivos temporales o generados por el compilador como, por ejemplo, ASP.NET.
- Opciones de memoria caché de análisis de vulnerabilidad: si está refinando el asesoramiento de una base de código escaneando iterativamente y añadiendo reglas personalizadas y luego volviendo a escanear sin cambiar el código fuente, puede reducir significativamente el tiempo de escaneo si establece las propiedades del proyecto de modo que utilice una caché de análisis de

vulnerabilidad. Para ello, marque el cuadro de selección **Habilitar memoria caché de análisis de vulnerabilidad** en las propiedades del proyecto. La primera vez que escanee el proyecto tras marcar este cuadro de selección, se creará una memoria caché de análisis de vulnerabilidad. Para cada siguiente escaneo del proyecto, se utilizará la memoria caché de análisis de vulnerabilidad y se reducirá el tiempo de escaneo.

Para borrar la caché de análisis de vulnerabilidad, y la caché que se crea cuando se ha habilitado el análisis incremental de Java, pulse **Borrar memoria caché**. La próxima vez que escanee un proyecto, tendrá lugar un escaneo completo y se creará una nueva caché de análisis de vulnerabilidad. Es posible que desee borrar la memoria caché si:

- El código fuente del proyecto se ha modificado desde el último escaneo.
- Ha realizado cambios en la configuración del proyecto, como por ejemplo añadir o suprimir archivos de origen.
- Ha cambiado las opciones de configuración del código fuente. Por ejemplo, puede que desee borrar la memoria caché si está escaneando Java y la vía de acceso de clase ha cambiado, o si está escaneando C o C++ y ha modificado la vía de acceso de inclusión o las definiciones de preprocesador.
- Ha habilitado el análisis incremental de Java y desea ejecutar un escaneo completo o se presentan problemas que pueden solucionarse borrando la caché. Consulte el apartado “Análisis incremental para Java” en la página 122 para obtener más información.

**Nota:** También puede borrar la memoria caché de análisis de vulnerabilidad marcando el cuadro de selección **Borrar memoria caché** al crear reglas personalizadas en el Asistente de reglas personalizadas.

- **Análisis de la cadena:** el análisis de la cadena supervisa la manipulación de cadenas en proyectos Java o Microsoft .NET. Proporciona la detección automática de rutinas de saneamiento y validación. Con esta detección se pueden reducir los falsos positivos y negativos. Marque el cuadro de selección **Habilitar análisis de la cadena para encontrar funciones validador/saneador** para habilitar el análisis de la cadena. El cuadro de selección **Aplicar las reglas importadas al ámbito global** determina si las rutinas de saneamiento o validación descubiertas se deben aplicar a un único proyecto o a nivel general (a todos los proyectos).

**Nota:** La aplicación del análisis de cadena puede ralentizar un escaneo. Por lo tanto, se recomienda que solo se aplique tras cambios en el código y luego se inhabilite para los siguientes escaneos. Además, las rutinas descubiertas se pueden ver como *sugerencias* y los auditores las pueden revisar. Estas rutinas se pueden ver en la vista Reglas personalizadas.

- **Codificación del archivo:** la codificación de caracteres de los archivos del proyecto debe establecerse de modo que AppScan Source pueda leer los archivos correctamente (y, por ejemplo, mostrarlos correctamente en la vista de origen).

**Nota:** La codificación del archivo predeterminado para proyectos AppScan Source es **ISO-8859-1**. La codificación de archivos predeterminada se puede cambiar en la página de preferencias generales.

## Filtros

Este separador permite especificar filtros existentes para el proyecto seleccionado, y la forma en que desea aplicar los filtros (un filtro se puede aplicar de forma directa o de forma inversa). Consulte Capítulo 5, “Selección y análisis”, en la página 145 para obtener información sobre los filtros y “Aplicación de filtros globalmente” en la página 168

la página 168 para obtener más detalles sobre cómo aplicarlos globalmente.

## Reglas de patrón y Conjuntos de reglas

Cuando selecciona un proyecto en la vista Explorador, el separador Reglas de patrón y Conjuntos de reglas de la vista Propiedades le permitirá añadir reglas de patrón y conjuntos de reglas que se aplicarán al escanear el proyecto. Si utiliza un escaneo basado en patrón, busca patrones de texto que desea que aparezcan como resultados. Las reglas individuales y los conjuntos de reglas se pueden aplicar a las aplicaciones y a los proyectos. Consulte “Personalización con reglas basadas en patrón” en la página 247 para obtener información sobre el análisis basado en patrones y “Aplicación de reglas de patrón y de conjuntos de reglas” en la página 254 para obtener más información sobre cómo aplicar reglas y conjuntos de reglas en la vista Propiedades.

## Extensiones de archivo

Este separador sirve para configurar o añadir extensiones de archivo válidas para el proyecto, para excluir archivos de los escaneos y para especificar extensiones como archivos web.

La sección **Extensiones de archivo** muestra una lista de las extensiones que se han establecido de forma global en la página de preferencias “Extensiones de archivo de proyecto” en la página 107 para el tipo de proyecto actual (las extensiones de archivo se pueden elegir para un tipo de proyecto diferente utilizando el menú **Conjunto de extensiones de archivo**). Si desea excluir una extensión de los escaneos del proyecto actual, selecciónela en la lista y pulse **Extensión excluida**. Esto hace que la extensión aparezca listada en la sección **Extensiones excluidas** del separador.

Para añadir una extensión adicional al proyecto, seleccione **Añadir extensión** en la sección **Extensiones adicionales** y, a continuación, especifique la extensión del archivo e indique si los archivos con la extensión se deben escanear, considerar como un archivo web o si se deben excluir.

Tabla 32. Valores de extensión de archivo

| Valor               | Descripción                                                           | Ejemplos de utilización                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Escanear o Asesorar | Incluir archivos con la extensión indicada en los análisis completos. | <ul style="list-style-type: none"><li>• Si se crea una extensión .xxx para proyectos Java y se marca como <b>Escanear</b> o <b>Asesorar</b>, los archivos que tengan esta extensión se compilarán y escanearán.</li><li>• Un archivo puede ser parte de un proyecto y no ser marcado como <b>Escanear</b> o <b>Asesorar</b> si no se debe compilar ni escanear (como por ejemplo, archivos de cabecera en C++). Estos archivos se deberían incluir en el proyectos, y se debería buscar en ellos durante el análisis basado en patrones.</li></ul> |

Tabla 32. Valores de extensión de archivo (continuación)

| Valor              | Descripción                                                                                                                                            | Ejemplos de utilización                                                                                                                                                                                                                                                                          |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Archivo web</b> | Marca los archivos con la extensión indicada para la compilación de JSP. Este valor permite que AppScan Source separe orígenes web de orígenes no web. | Si se crea una extensión .yyy para proyectos Java y se marca como un <b>Archivo web</b> , los archivos que tengan esta extensión se organizarán como orígenes web en los proyectos. Cuando AppScan Source prepare el análisis, estos archivos serán precompilados en clases para ser analizados. |
| <b>Excluir</b>     | No crear archivos de origen en el proyecto para archivos con la extensión indicada. No se escanearán los archivos con esta extensión.                  | Cree una extensión .zzz para los archivos que son necesarios para la compilación de proyectos, pero que no se necesitan incluir en el análisis.                                                                                                                                                  |

## Orígenes

Especifique los orígenes que se incluirán en el escaneo.

- Directorio de trabajo: la ubicación del archivo de proyecto de AppScan Source (ppf) y la base para todas las vías de acceso relativas.
- **Añadir raíz de origen** y **Elimina raíz de origen**: el separador Orígenes muestra las propiedades establecidas para el proyecto desde el Asistente de configuración de proyecto o definidas en el archivo ppf importado.

**Eliminar raíz de origen** sólo está disponible cuando se selecciona el icono **Raíz de origen**. Se utiliza para eliminar el directorio raíz de código de origen.

- Encontrar raíces del origen (solo proyectos Java): dejar que AppScan Source for Analysis busque automáticamente todas las raíces de origen válidas.
- Los archivos de proyecto se listan bajo el icono **Raíz de origen**. Los archivos que se excluyen del escaneo tienen un icono de archivo rojo (si se pulsa con el botón derecho del ratón sobre un archivo excluido, su menú tiene **Excluir** inhabilitado e **Incluir** habilitado). Para excluir un archivo incluido, pulse con el botón derecho del ratón sobre dicho archivo y elija **Excluir** en el menú. Para incluir un archivo excluido, pulse con el botón derecho del ratón sobre dicho archivo y elija **Incluir** en el menú.

## Dependencias del proyecto JavaServer Page (JSP)

El separador Dependencias del proyecto JSP muestra las propiedades establecidas para el proyecto JSP especificado.

- Contiene contenido (JSP) web: identifica si el proyecto es una aplicación web que contiene JavaServer Pages.
- Raíz de contexto web: un archivo WAR o un directorio que contiene el directorio WEB-INF. La raíz de contexto web debe ser la raíz de una aplicación web válida.
- Compilador de JSP: Tomcat 7, listo para utilizar, es el valor de compilador JSP predeterminado (el compilador JSP predeterminado se puede modificar en la página de preferencias de Java y JSP). Para conocer los compiladores a los que AppScan Source da soporte, consulte <http://www.ibm.com/support/docview.wss?uid=swg27027486>.

La instalación de AppScan Source incluye Apache Tomcat Versiones 7 y 8. Si las páginas de preferencias de **Tomcat 7** y **Tomcat 8** no están configuradas, AppScan Source compilará los archivos JSP mediante el compilador Tomcat JSP proporcionado que actualmente está marcado como predeterminado. Si desea utilizar un compilador Tomcat soportado externo, utilice la página de preferencias de Tomcat para apuntar a la instalación local de Tomcat.

Si utiliza un servidor de aplicaciones Oracle WebLogic Server o WebSphere Application Server, debe configurar la página de preferencias correspondiente para que apunte a la instalación local del servidor de aplicaciones a fin de que se pueda utilizar para la compilación de JSP durante el análisis. Si aún no ha finalizado esta configuración, se le solicitará mediante un mensaje el que lo haga cuando se seleccione el compilador JSP. Si pulsa **Sí** en el mensaje, se le llevará a la página de preferencias adecuada. Si pulsa **No**, un enlace de aviso aparecerá junto a la selección del compilador JSP (siguiendo dicho enlace se abrirá la página de preferencias).

## Dependencias del proyecto

El separador Dependencias del proyecto muestra propiedades del proyecto. Los valores de configuración en este separador varían según el lenguaje, por ejemplo:

- **Opciones** permite seleccionar los parámetros del compilador necesarios adicionales.
- Los valores de JDK son específicos de Java.
- Las definiciones de preprocesador son específicas del código C/C++. Al especificar definiciones de preprocesador, no incluya la opción -D del compilador (por ejemplo, especifique a=definition1 en lugar de -Da=definition1). Al especificar varios destinos, utilice una lista delimitada por puntos y comas.
- La configuración de destino sólo está disponible proyectos .NET y C++.

## Compilación

- Opciones: parámetros necesarios del compilador adicionales para la configuración del proyecto.
- Utilizar JDK: identificar el JDK utilizado para la compilación del proyecto, tal como está configurado en Preferencias. Consulte Capítulo 3, “Preferencias”, en la página 93.

Los proyectos Java pueden hacer referencia a una ubicación local de Java Development Kit (JDK). Cuando los proyectos se mueven al servidor, es posible que la vía de acceso de JDK deje de ser válida. Para transferir proyectos locales al servidor, debe identificar la vía de acceso de JDK predeterminada para cada proyecto que especifica un JDK con nombre.

**Nota:** El compilador predeterminado, listo para utilizar, para los proyectos JSP es Tomcat 7, y necesita Java Versión 1.6 o superior. Si se mantiene **Tomcat 7** como predeterminado, utilizar un JDK anterior provocará errores de compilación durante los escaneos.

- Validar: **Validar** asegura que las dependencias del proyecto estén correctamente configuradas. Comprueba los proyectos Java para ver si hay conflictos de configuración entre los orígenes y la vía de acceso de clase y si existen errores de compilación. **Existe un conflicto** si una clase de una vía de acceso de clase está duplicada en una raíz de origen. (Si existe un conflicto, modifique la vía de acceso de clase para eliminar la clase conflictiva.)

Después de comprobar si existen conflictos, **Validar** determina si el proyecto se compila y notifica cualquier error de compilación.

## Optimizaciones

- **Clases precompiladas:** utilice archivos de clases precompiladas Java o JSP en lugar de realizar la compilación durante el escaneo. Si está seleccionada, esta opción inhabilita las opciones de organización de orígenes.
- Organizar archivos de origen para minimizar los efectos de errores de compilación: controla si AppScan Source copia los orígenes en el directorio de organización.

**Corregir para que los paquetes no coincidan con la estructura de directorio** requiere que la compilación de Java abra cada archivo de origen.

**Limpiar el área de transferencia entre cada escaneo** aumenta el rendimiento entre escaneos.

## Separador Precompilar (solo ASP.NET)

La precompilación se consigue realizando una solicitud HTTP a una página especial (precompile.axd de forma predeterminada) del sitio web. Esta página la procesa un manejador de HTTP especial especificado en el archivo web.config. Este manejador compila todo el sitio, incluidos los archivos client.aspx, en el directorio de archivos ASP.NET temporal del directorio del sistema .NET, donde todos se escanean.

Para escanear ASP.NET 1.1, debe instrumentar el sitio web de modo que dicho sitio compile y genere información de depuración. Por lo tanto, el hecho de que un sitio web compile y genere información de depuración constituye, por sí mismo, una vulnerabilidad de seguridad. Puede pasar por alto tranquilamente esta vulnerabilidad puesto que el escaneo lo requiere. Sin embargo, asegúrese de que la aplicación desplegada no se compile con debug=true en web.config.

Para precompilar un sitio web ASP.NET 1.1, añada este elemento como hijo al elemento <system.web> en el archivo web.config:

```
<httpHandlers><add verb="*" path="precompile.axd"
type="System.Web.Handlers.BatchHandler"/></httpHandlers>
```

También debe establecer debug=true en el elemento de compilación. Por ejemplo:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <system.web>
    <httpHandlers><add verb="*" path="precompile.axd"
type="System.Web.Handlers.BatchHandler"/>
</httpHandlers>
    <compilation
      defaultLanguage="c#"
      debug="true"
    />
  </system.web>
</configuration>
```

Este elemento especifica al sitio web que la página precompile.axd será manejada por la clase .Net especial System.Web.Handlers.BatchHandler. Esta clase precompila el contenido del sitio web en el directorio de archivos ASP.NET temporal.

- Sitio web: destino de la solicitud para precompilar el sitio. La ubicación predeterminada es precompile.axd. Precompile.axd es un archivo virtual y se correlaciona con el archivo especificado en el archivo web.config.
- Directorio de salida: el directorio de destino de la precompilación. AppScan Source busca la salida en este directorio.
- Precompilar el sitio web ASP.NET: AppScan Source precompila y escanea automáticamente la salida precompilada durante un escaneo.



- Detener escaneo si falla la precompilación: si se selecciona **Precompilar el sitio web ASP.NET** y **Detener escaneo si falla la precompilación**, un escaneo se detiene si la precompilación falla. De lo contrario, el escaneo continúa únicamente en la salida primaria del sitio web.
- Compilar ahora: probar que la precompilación, basada en los valores actuales, se realiza correctamente antes de realizar el escaneo. La salida de la compilación se muestra en el panel Salida de la precompilación.
- Ensamblados adicionales: para cualquier tipo de proyecto .NET, especifique los ensamblados adicionales que desea escanear.
- Preferencias del proyecto: lista de los directorios en los que hay que buscar ensamblados a los que se hace referencia en proyectos de ensamblado .NET y proyectos .NET existentes.

### Propiedades de archivo

Las propiedades de archivo se parecen a las dependencias de proyecto y generalmente se configuran para aplicaciones C/C++.

Incluir datos de configuración desde proyecto: incluir los datos de configuración del proyecto en la configuración del archivo. La configuración del archivo consta entonces de la configuración acumulada del proyecto y de la configuración del archivo. La configuración de archivo prevalece sobre la configuración de proyecto.

## Vista Configuración del escaneo

La vista Configuración del escaneo le permite crear configuraciones que puede utilizar al iniciar escaneos. También puede utilizar la vista para establecer una configuración de escaneo predeterminada. En una configuración de escaneo, puede especificar las reglas de origen que se utilizan durante un escaneo y puede incluir varios valores de escaneo. Los valores establecidos en una configuración de escaneo a menudo pueden mejorar los resultados del escaneo, y la posibilidad de guardar estos valores facilita el escaneo y permite ahorrar tiempo.

La vista Configuración del escaneo tiene estas secciones principales:

- “Gestión de la configuración de escaneo” en la página 119
- “Separador General” en la página 120
- “Separador Análisis de flujo corrupto” en la página 120
- “Separador Análisis de patrones” en la página 121

### Gestión de la configuración de escaneo

Utilice esta sección para seleccionar, añadir, eliminar, guardar y compartir configuraciones de escaneo, así como para establecer configuraciones de escaneo predeterminadas.

- Para crear una nueva configuración de escaneo, pulse **Nueva**. Después de completar los valores de la configuración de escaneo, pulse **Guardar** para guardar los cambios. Para establecer la configuración de escaneo como el valor predeterminado, pulse **Seleccionar como valor predeterminado** después de guardarla. Para obtener más información sobre cómo se utiliza la configuración de escaneo predeterminada, consulte “Escaneo de código fuente” en la página 109.
- Para trabajar con una configuración de escaneo existente, selecciónela en la lista:
  - Si modifica los valores de la configuración de escaneo, pulse **Guardar** para guardar los cambios (para descartar los cambios no deseados, cambie a otra configuración de escaneo y pulse **Descartar**).

- Para eliminar la configuración de escaneo seleccionada, pulse **Suprimir**.
- Para duplicar la configuración de escaneo, pulse **Duplicar**. Se creará una nueva configuración de escaneo basada en los valores de la configuración de escaneo original.
- Para establecer la configuración de escaneo como el valor predeterminado, pulse **Seleccionar como valor predeterminado**. Para obtener más información sobre cómo se utiliza la configuración de escaneo predeterminada, consulte “Escaneo de código fuente” en la página 109.
- Para compartir la configuración de escaneo con otras personas, pulse **Compartir**. La configuración de escaneo se guardará en base de datos de AppScan Source.

**Nota:** Para compartir configuraciones de escaneo, o para modificar o suprimir una configuración de escaneo compartida, debe tener permiso para **Gestionar configuraciones compartidas**. Para obtener información sobre cómo establecer permisos, consulte el manual *IBM Security AppScan Source Guía de instalación y administración*.

**Nota:** AppScan Source proporciona configuraciones de escaneo incorporadas. Estas no se pueden modificar ni eliminar. Si las selecciona en la lista, podrá duplicarlas o ver sus valores.

## Separador General

### Información básica

Esta sección permite nombrar configuraciones de escaneo y proporcionar descripciones.

### Filtros

En esta sección, puede elegir uno o varios filtros para aplicar al escaneo, siempre que se utilice la configuración de escaneo. Al seleccionar un filtro, puede elegir un AppScan Source filtro predefinido o un filtro compartido o uno que haya creado. Consulte “Gestión de las configuraciones de escaneo” en la página 113 para ver más detalles.

## Separador Análisis de flujo corrupto

### Análisis de flujo corrupto

Habilite y establezca el ámbito del análisis de flujo corrupto.

### Reglas de escaneo

Utilice esta sección para determinar qué reglas de origen se aplicarán en el escaneo.

Un origen es una entrada para el programa, como un archivo, una solicitud de servlet, una entrada de consola o un socket. Al excluir algunas reglas de origen, puede acelerar el escaneo y evitar la detección de vulnerabilidades debidas a entradas que no son de interés.

Las reglas se etiquetan con propiedades de reglas para indicar que están relacionadas con una determinada vulnerabilidad, mecanismo, atributo o

tecnología. Estas propiedades se agrupan en conjuntos de reglas, que se corresponden con un conjunto común de reglas relacionadas. Puede limitar las reglas de origen incluidas en el escaneo mediante la especificación de conjuntos de reglas o propiedades de reglas individuales.

- Seleccione uno o varios tipos de vulnerabilidad (organizados por tipo en los conjuntos de reglas) que desee incluir en el escaneo:
  - **Todo:** si selecciona esta opción, se detectarán las vulnerabilidades debidas a todos los orígenes de entrada soportados.
  - **Entrada de usuario:** si selecciona esta opción, se detectarán las vulnerabilidades debidas a la entrada del usuario final.
  - **Aplicaciones web:** si selecciona esta opción, se detectarán las vulnerabilidades debidas al riesgo de las aplicaciones web.
  - **Registro y manejo de errores:** si selecciona esta opción, se detectarán las vulnerabilidades debidas a los mecanismos de registro y manejo de errores.
  - **Entorno:** si selecciona esta opción, se detectarán las vulnerabilidades debidas a los archivos de configuración, los archivos del entorno del sistema y los archivos de propiedades.
  - **Sistemas externos:** si selecciona esta opción, se detectarán las vulnerabilidades debidas a las entidades externas.
  - **Almacén de datos:** si selecciona esta opción, se detectarán las vulnerabilidades debidas a los almacenes de datos (por ejemplo, las bases de datos y la memoria caché).
  - **Elementos poco usuales:** si selecciona esta opción, se detectarán las vulnerabilidades debidas a las rutinas que no forman parte normalmente de una aplicación de producción.
  - **Sistema de archivos:** si selecciona esta opción, se detectarán las vulnerabilidades debidas a los sistemas de archivos.
  - **Datos confidenciales:** si selecciona esta opción, se detectarán las vulnerabilidades debidas a los datos confidenciales.

El texto flotante describe cada conjunto de reglas de esta sección.

- Seleccione las propiedades de las reglas de escaneo individuales que desee incluir en el escaneo: pulse **Descartar los conjuntos de reglas seleccionados y permitir seleccionar propiedades de regla individuales**. Esto abre el cuadro de diálogo Seleccionar propiedades de reglas, que le permite seleccionar las propiedades de la regla individual. Si se rellena este cuadro de diálogo, se descartarán los conjuntos de reglas que se hayan seleccionado. Las reglas de escaneo que tienen seleccionadas propiedades de regla se utilizarán para el escaneo.

## Valores avanzados

Esta sección está especialmente indicada para usuarios avanzados. Contiene una amplia variedad de valores que pueden mejorar los resultados del escaneo. El texto flotante describe cada valor de esta sección.

## Separador Análisis de patrones

### análisis de patrón

Utilice esta sección para habilitar el escaneo basado en patrones cuando se utilice la configuración de escaneo. El escaneo basado en patrones es un análisis del código fuente basado en criterios de búsqueda personalizados.

## Conjuntos de reglas de patrón y Reglas de patrón

Utilice estas secciones para añadir reglas y conjuntos de reglas a utilizar durante el análisis de patrones. Consulte los apartados “Personalización con reglas basadas en patrón” en la página 247 y “Gestión de las configuraciones de escaneo” en la página 113 para obtener más información.

## Editor de informe

Con el Editor de informes, puede editar informes o plantillas personalizados o crear un nuevo informe. Los informes personalizados incluyen elementos que están disponibles en un informe de resultados, tales como la información de los resultados, los fragmentos de códigos, el contenido de remediación y rastreo de AppScan Source, al igual que una matriz de vulnerabilidad. Antes de empezar a diseñar nuevos informes, se recomienda familiarizarse con el proceso de creación de informes, modificando una plantilla de informe existente en el Editor de informes.

El Editor de informes consta de los separadores Diseño de informe, Categorías y Vista previa.

- **Diseño de informe:** diseñar el aspecto del informe. En el diseño puede añadir, eliminar o reordenar elementos del informe de AppScan Source.
- **Categorías:** crear y editar categorías. Una *categoría* es un grupo de resultados. La categoría identifica los resultados que se deben incluir en el informe, cómo agrupar dichos resultados y el orden de agrupación.
- **Vista previa:** mirar el informe correspondiente al asesoramiento actual mientras se edita.

Los tres separadores contienen campos comunes:

- **Archivo:** vía de acceso del archivo de agrupación guardado (solo lectura). No se muestra nada en este campo hasta que se ha guardado el archivo. Una vez guardado, el archivo de agrupación es un archivo XML que define el informe.
- **Nombre:** nombre del informe definido por el usuario.

Los botones de la barra de herramientas para guardar, abrir, crear, copiar y generar informes personalizados incluyen:

- **Crear un nuevo informe:** crea un nuevo informe personalizado
- **Nuevo informe a partir de uno existente:** crea un nuevo informe personalizado a partir de una plantilla de informe existente
- **Abrir un informe guardado:** abre un archivo de agrupación para editarlo
- **Guardar:** guarda el informe actual en el archivo especificado
- **Guardar como:** guarda el informe actual en un archivo nuevo
- **Generar una instancia de este informe:** crea una copia del informe para el asesoramiento actualmente abierto

**Consejo:** Para ver ejemplos de informes existentes, pulse **Nuevo informe a partir de uno existente** y, a continuación, elija una de las plantillas de informes de AppScan Source. Si explora los separadores Diseño de informe y Categorías en las plantillas puede ver cómo están diseñados los informes.

### Separador Diseño de informe

El separador Diseño de informe consta de las secciones Paleta y de secciones que le permiten especificar una cabecera o pie de página que aparecerá en cada página.

## Cabecera de página y Pie de página

El campo **Cabecera de página** le permite especificar el texto que aparece en la parte superior de cada página de un informe y el campo **Pie de página** le permite especificar el texto que aparece en la parte inferior de cada página.

## Paleta

La Paleta muestra una lista de elementos que comprenden los informes estándares de AppScan Source. Algunos de los elementos sólo muestran información para las categorías que se han definido en el separador Categorías (consulte la sección Tabla 19 en la página 233).

*Tabla 33. Paleta de diseño de informe: los elementos que no dependen de las categorías*

| Elemento del informe       | Descripción                                                                                                                                     |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Cabecera de texto          | Añade un bloque de texto en negrita al diseño de informe.                                                                                       |
| Cabecera de imagen         | Muestra una imagen escalada a un tamaño especificado en píxeles.                                                                                |
| Cabecera de AppScan Source | Cabecera de informe que contiene información de marca de AppScan Source.                                                                        |
| Título y fecha             | Título de informe que incluye el nombre del elemento que se ha escaneado, junto con la fecha de escaneo y la fecha en que se generó el informe. |
| Bloque de texto            | Cualquier texto definido por el usuario. Una cabecera también se puede añadir para el bloque de texto en el campo <b>Etiqueta</b> .             |
| Matriz de vulnerabilidad   | Matriz de vulnerabilidad del asesoramiento (muestra el mismo gráfico que aparece en la vista Matriz de vulnerabilidad).                         |
| Métricas                   | Identifica el número total de paquetes, clases, métodos y líneas de código de todos los paquetes del proyecto.                                  |
| Historial de escaneo       | Métricas para el escaneo actual y métricas históricas para escaneos del mismo destino.                                                          |

*Tabla 34. Paleta de diseño de informe: elementos que dependen de categorías*

| Elemento del informe       | Descripción                                                                                                                                                                                      |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tarjeta de informe         | Breve desglose de niveles de vulnerabilidad de cada categoría definida en el separador Categorías. Contiene enlaces a los detalles del informe e indicadores de gravedad que resumen la sección. |
| Desglose de vulnerabilidad | Tabla con un desglose del número de vulnerabilidades en todas las categorías definidas en el separador Categorías, por gravedad y clasificación.                                                 |
| Tarjeta de informe parcial | Desglose de niveles de vulnerabilidad de categorías especificadas por el usuario como se ha especificado en el separador Categorías.                                                             |

Tabla 34. Paleta de diseño de informe: elementos que dependen de categorías (continuación)

| Elemento del informe | Descripción                                                                                                 |
|----------------------|-------------------------------------------------------------------------------------------------------------|
| Categorías           | Lista todos los datos de resultados categorizados, tal como se han especificado en el separador Categorías. |
| Categoría            | Lista todos los resultados en una o más categorías que se han definido en el separador Categorías.          |

## Diseño

A medida que añade elementos de la paleta, aparecen en el diseño. Utilice la barra de herramientas de la sección para eliminar, modificar o mover elementos en el diseño.

### Separador Categorías

Mediante el separador Categorías, puede añadir categorías que contienen resultados basados en paquetes, propiedades, o los resultados seleccionados que seleccione. A continuación, se pueden utilizar las categorías cuando se añaden determinados elementos al diseño. Por ejemplo, cuando añade un Desglose de vulnerabilidad al diseño, se añade al diseño una tabla con un desglose del número de vulnerabilidades en todas las categorías (por gravedad y clasificación). El separador Categorías consta de un panel con un árbol de categorías y un panel en el que se pueden editar los atributos de la categoría seleccionada. Cada categoría contiene los resultados del asesoramiento que satisfacen ciertos requisitos definidos por el usuario.

Las categorías disponibles incluyen:

- **Paquete:** la categoría de paquete consta de una lista de nombres de paquete. Cualquier resultado de un paquete cuyo nombre aparece en la lista aparece en esta categoría. Aunque se eligen paquetes procedentes del asesoramiento actual, puede aplicar la categoría de paquete a cualquier asesoramiento, puesto que los paquetes se comparan por nombre.
- **Resultados individuales:** elija los resultados específicos que desea añadir a la categoría. Al informe solo se añade una instantánea del resultado. Si modifica el resultado después de añadirlo al informe, este no refleja el campo.
- **Propiedades Tipos de vulnerabilidad, Mecanismos y Tecnologías:** seleccione conjuntos de propiedades y propiedades necesarias de las API de la Base de datos de conocimientos de AppScan Source Security. Si un resultado contiene al menos una de las **Propiedades** y todas las **Propiedades necesarias**, se incluye en el informe.

Esta tabla identifica los paneles de categorías y los elementos de que consta el panel.

Tabla 35. Atributos del separador Categorías

| Atributo                                              | Descripción                                                                                                                                                                                                                    | Cómo editarlo                                                                                                                                                                                     |
|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Etiqueta                                              | El nombre abreviado de la categoría, por ejemplo, Desbordamiento de almacenamiento intermedio. La etiqueta identifica la categoría en la lista de árbol de categorías y es la cabecera de categoría del informe personalizado. | Escriba una etiqueta en un campo de texto de una sola línea.                                                                                                                                      |
| Resumen                                               | Una plantilla para una frase que indique cuántos resultados se notifican en esta categoría. El recuento real sustituye %FindingCount% durante la generación del informe.                                                       | Escriba una breve descripción de la categoría y pulse <b>Añadir cuenta</b> para colocar la variable %FindingCount% en la frase en la posición del cursor.                                         |
| Texto                                                 | Breve descripción de la categoría.                                                                                                                                                                                             | Especifique el texto que describe la categoría.                                                                                                                                                   |
| Propiedades (solo categorías de propiedad)            | Los resultados que tengan al menos una de estas propiedades se notificarán en esta categoría. Si un resultado no tiene todas las propiedades necesarias listadas, el resultado no se incluye en esta categoría.                | Pulse <b>Añadir</b> en la barra de herramientas y seleccione una propiedad del cuadro de diálogo Añadir propiedades. Pulse <b>Eliminar</b> para eliminar de la lista los elementos seleccionados. |
| Propiedades necesarias (solo categorías de propiedad) | Los resultados que tienen todas las propiedades necesarias y al menos una propiedad aparecen en el informe bajo esta categoría.                                                                                                | Pulse <b>Añadir</b> en la barra de herramientas y seleccione una propiedad del cuadro de diálogo Añadir propiedades. Pulse <b>Eliminar</b> para eliminar de la lista los elementos seleccionados. |
| Paquetes (solo categorías de paquete)                 | Especifica los nombres de los paquetes que se deben incluir en esta categoría.                                                                                                                                                 | Pulse <b>Añadir un paquete</b> en la sección Paquetes y seleccione los paquetes en la lista.                                                                                                      |

Tabla 35. Atributos del separador Categorías (continuación)

| Atributo                                      | Descripción                                                       | Cómo editarlo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Resultados (solo de categorías de resultados) | Especifica los resultados que se deben incluir en esta categoría. | <p>Seleccione los resultados de cualquier tabla de resultados y, a continuación, pulse <b>Añadir resultados</b> en la barra de herramientas de la tabla para añadir los resultados seleccionados. Si más de una vista contiene los resultados seleccionados, se le solicitará que seleccione la vista que contiene los resultados seleccionados que desea añadir.</p> <p>También puede arrastrar los resultados de una tabla de resultados a la tabla de la vista Editor de informes, en el Editor de informes o directamente a una categoría de resultados existente del árbol de categorías.</p> |

### Separador Vista previa

Puede realizar una vista previa de los informes de AppScan Source for Analysis a medida que edita sus plantillas. En el panel Vista previa, pulse **Vista previa** para ver el informe correspondiente a un asesoramiento abierto.

## Vistas que ayudan con la salida de escaneo

Las vistas en esta sección se utilizan para la visualización y la gestión de la salida de escaneo.

- “Vista Consola”
- “Vista Métricas” en la página 313
- “Vista Mis asesoramientos” en la página 313
- “Vista Asesoramientos publicados” en la página 314

### Vista Consola

La vista Consola muestra la salida correspondiente al escaneo actual, incluida información de estado, texto de salida y mensajes de error. La vista puede mostrar dos consolas, una para el escaneo que se está ejecutando actualmente y una para el escaneo completado.

Una consola de salida muestra la salida completa del escaneo, incluidos los archivos escaneados, el número total de archivos escaneados, el número total de vulnerabilidades que se han encontrado y la densidad de vulnerabilidad.

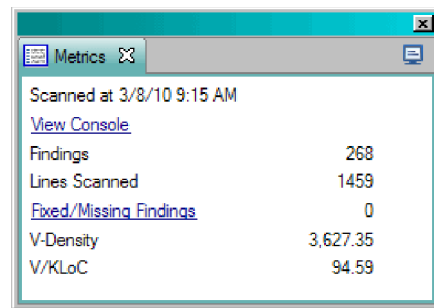
Los botones de la barra de herramientas manipulan la salida de la consola.

Una consola de errores muestra los mensajes de error de salida y el número de errores del escaneo. El valor de los errores se actualiza durante el escaneo.



## Vista Métricas

La vista Métricas presenta estadísticas por asesoramiento e incluye líneas de código escaneadas, número total de resultados, Densidad-V, y V/KLoC.



The screenshot shows a window titled 'Metrics' with a close button. Inside, it displays the scan date and time, a link to 'View Console', and a table of statistics.

|                                        |          |
|----------------------------------------|----------|
| Scanned at 3/8/10 9:15 AM              |          |
| <a href="#">View Console</a>           |          |
| Findings                               | 268      |
| Lines Scanned                          | 1459     |
| <a href="#">Fixed/Missing Findings</a> | 0        |
| V-Density                              | 3,627.35 |
| V/KLoC                                 | 94.59    |

## Vista Consola

Hiperenlace que abre la vista Consola para ver la salida del escaneo actual.

## Resultados

Número de resultados identificados por el escaneo.

## Líneas escaneadas

Número de líneas de código escaneadas.

## Resultados solucionados/ausentes

Número de elementos contenidos en los paquetes de aplicación pero no encontrados en este escaneo.

## Densidad-V

Expresión numérica que proporciona una forma coherente de evaluar la vulnerabilidad de sus aplicaciones. La densidad-V se calcula relacionando el número e importancia crítica de los resultados con el tamaño de la aplicación o proyecto que se analiza.

## V/KLoC

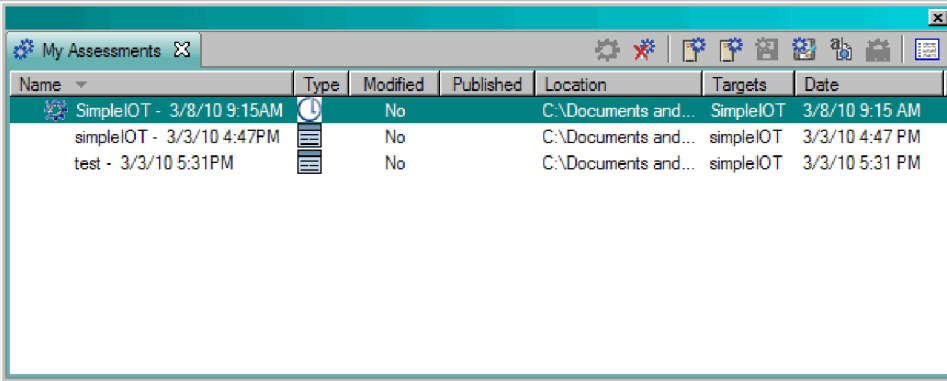
Vulnerabilidades encontradas por cada mil líneas de código.

## Vista Mis asesoramientos

La vista Mis asesoramientos contiene una lista de asesoramientos (el asesoramiento abierto actualmente, junto con otros asesoramientos que ha guardado). Si se modifica el conjunto de trabajo actual de asesoramientos (por ejemplo, si añade un nuevo asesoramiento o modifica un asesoramiento), un asterisco junto al título de vista indica que hay cambios no guardados en el conjunto de trabajo.

- **Nombre:** nombre del asesoramiento.
- **Tipo:** icono que indica que el escaneo ha cubierto aplicaciones (🔍), proyectos (📁) o archivos (📄). Una estrella junto al nombre del asesoramiento indica que el asesoramiento está abierto actualmente.
- **Configuración de escaneo:** Configuración de escaneo que se utilizó para el escaneo.

- **Modificado:** Sí o No indica el estado modificado del asesoramiento.
- **Publicado:** indicador de que los asesoramientos se han publicado en la base de datos de AppScan Source.
- **Ubicación:** vía de acceso al archivo de asesoramiento (<nombre\_archivo>.ozasmt).
- **Destinos:** aplicaciones, proyectos o archivos escaneados.
- **Fecha:** fecha de finalización del escaneo.



| Name                      | Type | Modified | Published | Location            | Targets   | Date           |
|---------------------------|------|----------|-----------|---------------------|-----------|----------------|
| SimpleIoT - 3/8/10 9:15AM |      | No       |           | C:\Documents and... | SimpleIoT | 3/8/10 9:15 AM |
| simpleIoT - 3/3/10 4:47PM |      | No       |           | C:\Documents and... | simpleIoT | 3/3/10 4:47 PM |
| test - 3/3/10 5:31PM      |      | No       |           | C:\Documents and... | simpleIoT | 3/3/10 5:31 PM |

Cuando finalizan los escaneos, aparecen automáticamente en la vista Mis asesoramientos. Los asesoramientos visibles en esta vista incluyen escaneos realizadas desde este sistema o las que el usuario ha añadido.

En esta vista, puede abrir, añadir, eliminar, publicar, guardar, renombrar o comparar asesoramientos. Si elimina un asesoramiento de esta vista sin guardarlo ni publicarlo, se suprime de forma permanente. Tenga en cuenta que cada asesoramiento guardado incluye todos los resultados, la salida y los registros de errores. Consulte “Guardar asesoramientos” en la página 139 para ver detalles sobre cómo guardar y publicar asesoramientos.

Consulte “Comparación de dos asesoramientos en la vista Diferencia entre asesoramientos” en la página 182 para ver más detalles sobre cómo comparar asesoramientos.

**Consejo:** La preferencia **General** establece el número máximo de asesoramientos que se visualizarán en las vistas Asesoramientos publicados y Mis asesoramientos.

## Vista Asesoramientos publicados

La vista de Asesoramientos publicados muestra una lista de los asesoramientos que se han publicado para la base de datos de AppScan Source.

- **Nombre:** nombre del asesoramiento.
- **Tipo:** icono que indica que el escaneo ha cubierto aplicaciones () , proyectos () o archivos (). Una estrella junto al nombre del asesoramiento indica que el asesoramiento está abierto actualmente.
- **Configuración de escaneo:** Configuración de escaneo que se utilizó para el escaneo.
- **Publicador:** nombre de usuario de la persona que ha publicado el asesoramiento.
- **Destinos:** aplicaciones, proyectos o archivos escaneados.
- **Fecha:** fecha de finalización del escaneo.

En la vista Asesoramientos publicados, puede ver:

- Añadir asesoramientos a la vista mis asesoramientos
- Filtrar asesoramientos
- Abrir y suprimir asesoramientos
- Cerrar asesoramientos
- Comparar asesoramientos
- Guardar asesoramientos
- Renombrar asesoramientos
- Ver métricas

**Consejo:** La preferencia **General** establece el número máximo de asesoramientos que se visualizarán en las vistas Asesoramientos publicados y Mis asesoramientos.

---

## Vistas que ayudan con la selección

Las vistas en esta sección se utilizan para la visualización y la gestión de una salida de escaneo precisa.

- “Vista Diferencia entre asesoramientos”
- “Vista Resultados personalizados” en la página 316
- “Vista Resultados excluidos” en la página 321
- “Vista Resultados” en la página 318
- “Vista Resultados solucionados/Ausentes” en la página 322
- “Vista Resultados modificados” en la página 321
- “Vista Resultados de la búsqueda” en la página 322
- “Vista de informe” en la página 322
- “Vista Entradas y salidas” en la página 325

### Vista Diferencia entre asesoramientos

La vista Diferencia entre asesoramientos representa una combinación de la vista Mis asesoramientos y la vista Resultados. Cuando selecciona dos asesoramientos para compararlos, se muestran las diferencias entre los dos asesoramientos.

En esta vista puede ver el número total de resultados nuevos, solucionados/que faltan y comunes.

- Los resultados comunes aparecen en ambos asesoramientos
- Los resultados nuevos son aquellos que solo aparecen en el más reciente de los dos asesoramientos (resaltado en azul)
- Los resultados solucionados/que faltan son los resultados que solo aparecen en el asesoramiento más antiguo (resaltado en cursiva y en verde)

El panel derecho muestra los resultados. Pulse con el botón derecho en un resultado de la tabla para:

- Generar un Informe de resultados
- Enviar los resultados como defectos
- Abrir en un editor externo
- Abrir en el editor interno

El panel izquierdo muestra los asesoramientos que se van a comparar.

**Nota:** La vista Diferencia entre asesoramientos pasa por alto los filtros.

## Vista Resultados personalizados

La vista Resultados personalizados muestra los resultados definidos por el usuario o *resultados personalizados* que existen en el asesoramiento abierto actualmente. En esta vista, puede crear, suprimir y modificar resultados personalizados para el asesoramiento actual. Cuando se crea un resultado personalizado en la vista Resultados personalizados, el nuevo resultado se añade al asesoramiento actual, y las métricas de asesoramiento se actualizan.

Los filtros y los paquetes no afectan a los resultados de la vista Resultados personalizados. En esta vista, no es posible ver los resultados del informe personalizado ni guardar los resultados seleccionados.

## Vistas con resultados

Muchas vistas de AppScan Source for Analysis contienen resultados:

- Vista Resultados
- Vista Resultados modificados
- Vista Resultados personalizados
- Vista Resultados excluidos
- Vistas de paquetes
- Vista Resultados solucionados/Ausentes
- Vista de informe
- Vista Resultados de la búsqueda
- Vista Diferencia entre asesoramientos

## Tabla Resultados

En esta tabla se describen las columnas disponible en las tablas de resultados. Si una columna no está disponible, es probable que esté oculta en la tabla. Para seleccionar la columna que desea visualizar (o realizar cualquier otra tarea de personalización en una tabla), siga las instrucciones de apartado “Personalizar la tabla de resultados” en la página 318.

*Tabla 36. Tabla Resultados*

| Cabecera de columna | Descripción                                                                              |
|---------------------|------------------------------------------------------------------------------------------|
| Rastreo             | Un icono en esta columna indica que existe un rastreo para salidas perdidas o conocidas. |

Tabla 36. Tabla Resultados (continuación)

| Cabecera de columna    | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gravedad               | <ul style="list-style-type: none"> <li>• <b>Alta</b> : Supone un riesgo para la confidencialidad, integridad o disponibilidad de los datos o la integridad o disponibilidad de los recursos de proceso. A las condiciones de gravedad alta debe dárseles prioridad para su remediación inmediata.</li> <li>• <b>Media</b> : Supone un riesgo para la seguridad de los datos o la integridad de los recursos, pero la condición es menos susceptible de ser atacada. Las condiciones de seguridad media deben revisarse y resolverse cuando sea posible.</li> <li>• <b>Baja</b> : Supone un riesgo mínimo para la seguridad de los datos o la integridad de los recursos.</li> <li>• <b>Información</b> : El resultado, en sí mismo, no es susceptible de ser comprometido. Sino que describe las tecnologías, las características de la arquitectura o los mecanismos de seguridad utilizados en el código.</li> </ul> |
| Clasificación          | <p>Tipo de resultado: resultado de seguridad <b>Definitivo</b> o <b>Sospechoso</b> o resultado de <b>Cobertura de escaneo</b>.</p> <p><b>Nota:</b> En algunos casos, se puede utilizar una clasificación de <b>Ninguno</b> para denotar una clasificación que no corresponde a un resultado de seguridad ni a un resultado de cobertura de escaneo.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Tipo de vulnerabilidad | Categoría de vulnerabilidad, como por ejemplo <code>Validation.Required</code> o <code>Injection.SQL</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| API                    | La llamada vulnerable, mostrando la API y los argumentos que se le pasan.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Fuente                 | Un origen es una entrada para el programa, como un archivo, una solicitud de servlet, una entrada de consola o un socket. En la mayoría de los orígenes de entrada, los datos devueltos son ilimitados en términos de contenido y longitud. Cuando se deselecta una entrada, se considera que está corrupta.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Receptor               | Una salida puede tener cualquier formato externo en el que puedan escribirse datos. Como ejemplo de salida cabe citar las bases de datos, los archivos, la salida de la consola y los sockets. Escribir datos en una salida sin verificarla puede ser indicio de una grave vulnerabilidad de seguridad.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Directorio             | Vía de acceso completa de los archivos escaneados.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

Tabla 36. Tabla Resultados (continuación)

| Cabecera de columna | Descripción                                                                                                                                                                                                                      |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Archivo             | Nombre del archivo de código donde se presenta el resultado de cobertura de escaneo o el resultado de seguridad. Las vías de acceso de archivos en los resultados son relativas al directorio de trabajo del proyecto escaneado. |
| Método de llamada   | La función (o método) desde la que se realiza la llamada vulnerable.                                                                                                                                                             |
| Línea               | Número de línea en el archivo de código que contiene la API vulnerable.                                                                                                                                                          |
| Paquetes            | Paquete que contiene este resultado.                                                                                                                                                                                             |
| CWE                 | ID y tema del diccionario desarrollado por la comunidad que recoge las debilidades comunes del software (temas de CWE (Common Weakness Enumeration)).                                                                            |

### Personalizar la tabla de resultados:

En todas las vistas con resultados, excepto la de Asesoramiento de diferencias en AppScan Source for Analysis, puede personalizar la tabla de resultados identificando qué columnas desea ver y en qué orden. Cada vista puede tener valores diferentes, o puede aplicar sus opciones a todas las vistas. Para personalizar el orden de las columnas, siga los pasos de este tema de tarea.

### Acerca de esta tarea

Para aprender sobre las columnas de una tabla de resultados, consulte “Tabla Resultados” en la página 316.

### Procedimiento

1. Pulse en el botón de la barra de herramientas **Seleccionar y ordenar columnas**.

**Nota:** En AppScan Source for Development (plugin de Visual Studio), pulse el botón de la barra de herramientas **Seleccionar y ordenar columnas de tabla**.

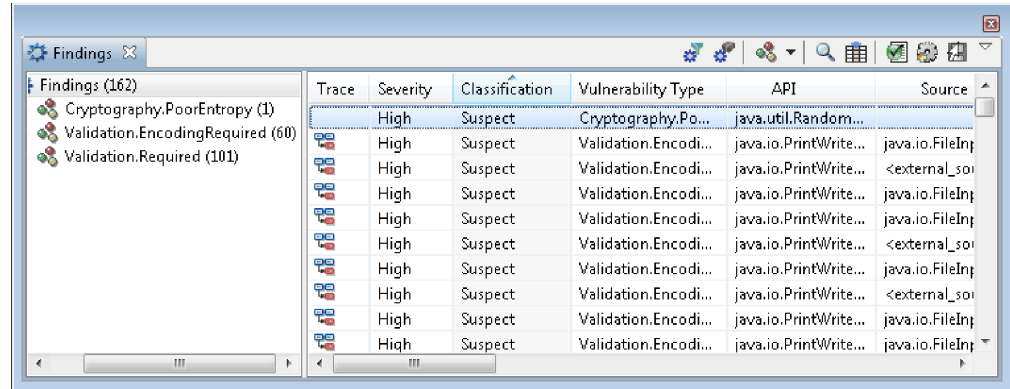
2. En el diálogo **Seleccionar y ordenar columnas**, seleccione el nombre de la columna y pulse la **Flecha arriba** o la **Flecha abajo** para mover la ubicación de la columna.
3. Pulse el botón **Añadir columna** para añadir una columna a la vista. También puede pulsar el botón **Suprimir columna** para eliminar una columna de la vista.

**Nota:** En AppScan Source for Development (plugin de Visual Studio), estos botones están etiquetados con **Insertar** y **Eliminar**, respectivamente.

4. Pulse **Restaurar valores predeterminados** para restablecer las columnas predeterminadas y el orden de columnas.
5. Pulse en **Aceptar** para guardar los valores.

### Vista Resultados

La vista Resultados contiene datos de los resultados de un asesoramiento. Los resultados se pueden agrupar por parámetros listados en este tema.



**Recuerde:** En AppScan Source for Development (plugin de Eclipse) y AppScan Source for Analysis, se conocen como *vistas* en la interfaz de usuario. En AppScan Source for Development (plugin de Visual Studio), se denominan *ventanas* en la interfaz de usuario. En esta documentación, el término *vista* generalmente se utiliza para hacer referencia tanto a *vistas* como *ventanas*.

## Agrupaciones de parámetros en la tabla de resultados

En la vista Resultados, seleccione la flecha hacia abajo del botón de la barra de herramientas **Seleccionar una jerarquía de árbol** y, a continuación, seleccione el parámetro por el que agrupar los resultados.

Tabla 37. Agrupaciones de parámetros en la tabla de resultados

| Modo                   | Agrupación                            |
|------------------------|---------------------------------------|
| Tipo de vulnerabilidad | Tipo, Gravedad, Clasificación         |
| Clasificación          | Clasificación, Gravedad, Tipo         |
| Archivo                | Proyecto, Directorio, Archivo, Método |
| API                    | API, Tipo                             |
| Paquetes               | Paquete, Tipo, API                    |
| CWE                    | CWE                                   |
| Tabla                  | No agrupar                            |

## Botones de la barra de herramientas

Tabla 38. Botones de la barra de herramientas

| Acción                                            | Icono | Descripción                                                                                         |
|---------------------------------------------------|-------|-----------------------------------------------------------------------------------------------------|
| Mostrar resultados que no coincidan con el filtro |       | Este botón le permite conmutar la visualización de los resultados filtrados en la vista Resultados. |

Tabla 38. Botones de la barra de herramientas (continuación)

| Acción                                    | Icono                                                                               | Descripción                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Mostrar resultados empaquetados</b>    |    | Este botón le permite conmutar la visualización de los resultados empaquetados en la vista Resultados. Esta acción oculta los resultados en todos los paquetes empaquetados que ha creado. Este valor no afecta a la visualización de resultados en paquetes excluidos. Estos resultados nunca se muestran en la vista Resultados. |
| <b>Seleccionar una jerarquía de árbol</b> |                                                                                     | Varía en función de la agrupación que se ha seleccionado.                                                                                                                                                                                                                                                                          |
| <b>Buscar</b>                             |    | Este botón abre un cuadro de diálogo que le permite buscar resultados. Una variedad de opciones de búsqueda están disponibles en este cuadro de diálogo. Después realizar una búsqueda, los resultados aparecen en la vista Resultados de la búsqueda.                                                                             |
| <b>seleccionar y ordenar columnas</b>     |  | Este botón abre el cuadro de diálogo Seleccionar y ordenar columnas, que le permite añadir o eliminar columnas, o modificar columnas existentes.                                                                                                                                                                                   |
| <b>Vista del informe</b>                  |  | Este botón abre la vista Informes, que muestra los resultados de acuerdo con informes de auditoría completos que calibran la conformidad con las prácticas recomendadas sobre seguridad de software y los requisitos reguladores.                                                                                                  |
| <b>Crear resultado personalizado</b>      |  | Este botón solo está disponible en AppScan Source for Analysis. Al seleccionando se abre el cuadro de diálogo Crear resultado personalizado, que le permite añadir un resultado personalizado al asesoramiento actual.                                                                                                             |



Tabla 38. Botones de la barra de herramientas (continuación)

| Acción                                  | Icono                                                                             | Descripción                                                                                                                                                                                              |
|-----------------------------------------|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Guardar resultados seleccionados</b> |  | Al seleccionar uno o varios resultados, este botón abre el cuadro de diálogo Guardar resultados seleccionados, que le permite guardar los resultados seleccionados en un nuevo archivo de asesoramiento. |
| <b>Menú Ver</b>                         |                                                                                   | Este menú proporciona un rápido acceso a todas las acciones de botón de la barra de herramientas.                                                                                                        |

En la vista Resultados, puede:

- Abrir el resultado en el editor de código
- Crear exclusiones
- Modificar resultados
- Visualizar resultados bajo diferentes agrupaciones
- Buscar elementos específicos en los resultados

Si utiliza la vista en AppScan Source for Analysis, también puede hacer lo siguiente:

- Mover resultados a un paquete
- Crear defectos en un sistema de seguimiento de defectos
- Crear resultados personalizados
- Generar informes de resultados
- Enviar resultados y paquetes por correo electrónico

### Vista Resultados excluidos

La vista Resultados excluidos contiene sólo resultados excluidos. Un resultado excluido es un resultado que omite de los escaneos. En esta vista puede buscar resultados específicos. Las columnas de esta vista son idénticas a las de la vista Resultados.

Para volver a incluir los resultados que se han excluido, siga las instrucciones de “Volver a incluir resultados que se han marcado como exclusiones” en la página 171.

### Vista Resultados modificados

La vista Resultados modificados contiene todos los resultados modificados de la aplicación actual. Los *resultados modificados* son resultados con el tipo de vulnerabilidad, gravedad, clasificación o notas alterados. Los *resultados perdidos* (resultados que no están en el asesoramiento abierto actualmente) aparecen en letra cursiva verde y no pueden modificarse.

En esta vista puede:

- Buscar resultados específicos.
- Realizar modificaciones adicionales

En AppScan Source for Analysis, también puede realizar las siguientes acciones en esta vista:

- Añadir resultados a paquetes
- Crear defectos en un sistema de seguimiento de defectos
- Enviar resultados (defectos) por correo electrónico
- Generar informes de resultados

### **Vista Resultados solucionados/Ausentes**

La vista Resultados solucionados/Ausentes identifica resultados que están en paquetes pero no en el asesoramiento actual. Un resultado se identifica como solucionado/ausente porque se ha resuelto o eliminado, o el archivo fuente no se ha escaneado.

### **Vista Resultados de la búsqueda**

Al buscar resultados, los resultados aparecen en la vista Resultados de la búsqueda.

En esta vista, puede hacer lo siguiente:

- Ordenar los resultados
- Editar código en un editor interno o externo
- Establecer el tipo de vulnerabilidad
- Ascender resultados de cobertura de escaneo y sospechosos a definitivos
- Establecer el nivel de gravedad
- Anotar resultados
- Excluir resultados específicos
- Realizar búsquedas posteriores

Si utiliza la vista en AppScan Source for Analysis, también puede hacer lo siguiente:

- Añadir resultados a paquetes
- Enviar defectos a sistemas de rastreo de defectos o enviar los resultados por correo electrónico
- Generar informes de resultados

La vista Resultados de la búsqueda contiene sólo los elementos que coinciden con los criterios de búsqueda y mantiene como máximo cinco resultados de búsqueda. Por ejemplo, si busca en la vista Resultados de la búsqueda un tipo de vulnerabilidad o un desbordamiento de almacenamiento intermedio, y luego busca una clasificación de definitivos, el resultado de la búsqueda se encuentra en la intersección de ambas búsquedas.

Los criterios de búsqueda aparecen en el campo de búsqueda, como representación de la búsqueda como "<palabra\_clave>" en <vista\_origen>: <campos buscados>, como por ejemplo, "cerrar" en Resultados [Contexto, API, Método]. Si cierra el asesoramiento actual, todos los resultados de la búsqueda se descartan y el campo de búsqueda contiene el texto Sin búsqueda actual.

### **Vista de informe**

La vista Informes le permite organizar los resultados de un escaneo según diversos informes de auditoría que calibran la conformidad con las prácticas recomendadas sobre seguridad de software y los requisitos reguladores.

La vista muestra los resultados según estos informes:

- “Informe de CWE/SANS Top 25 2011” en la página 227
- “Informe DISA Application Security and Development STIG V3R10” en la página 228
- “Informe Web Application Security Project (OWASP) Mobile Top 10” en la página 228
- “Informe Web Application Security Project (OWASP) Top 10 2013” en la página 228
- “Informe de Payment Card Industry Data Security Standard (PCI DSS) Versión 3.2” en la página 228
- “Informe de Software Security Profile” en la página 228

Si utiliza AppScan Source for Analysis para crear un informe personalizado que se guarda en <data\_dir>\reports\profile (donde <data\_dir> es la ubicación de los datos de programa AppScan Source, como se describe en “Instalación y ubicaciones de archivo de datos de usuario” en la página 335), también puede utilizar la vista Informes para visualizar los resultados por informe personalizado.

Las columnas en la vista de Informes son idénticas a las de “Vista Resultados” en la página 318.

## Búsqueda de resultados

En varias vistas que contienen resultados, puede buscar resultados específicos. El criterio de búsqueda incluye paquetes, código, archivos, proyectos y tipos de vulnerabilidad. Los resultados de la búsqueda aparecen en la vista Búsqueda de resultados.

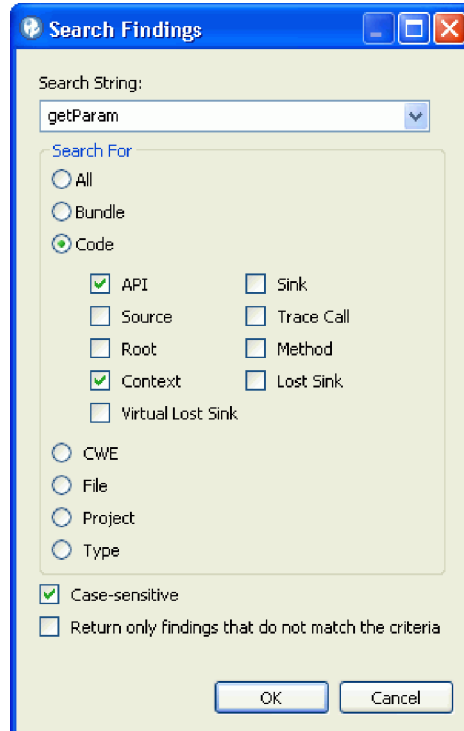
Cuando se busca código, la búsqueda puede realizarse por varios o por todos los elementos, incluyendo:

- API
- Contexto
- Método
- Fuente
- Receptor
- Receptor perdido
- Raíz
- Llamada de rastreo

**Buscar todas las apariciones de un elemento en todos los resultados:**

### Procedimiento

1. Seleccione la vista en la que buscar.
2. Seleccione **Editar > Buscar** en el menú principal (en AppScan Source for Development (plugin de Eclipse), seleccione **Editar > Buscar/Reemplazar** o en AppScan Source for Development (plugin de Visual Studio), pulse el botón **Buscar** en una vista con resultados).



3. Escriba una serie de búsqueda en el cuadro de diálogo **Buscar resultados**.
4. Busque la serie en un **Paquete, Código, CWE, Archivo, Proyecto, Tipo, o Todos**. Los resultados coincidentes aparecen en la vista Búsqueda de resultados. Seleccione **Distinguir mayúsculas de minúsculas** para buscar texto teniendo en cuenta la diferencia entre mayúsculas y minúsculas.  
Si utiliza AppScan Source for Analysis o AppScan Source for Development (plug-in de Eclipse), seleccione **Devolver sólo resultados que no coincidan con los criterios** para obtener sólo los resultados que no correspondan a los criterios de búsqueda.

#### Búsqueda de resultados en una tabla de resultados:

##### Procedimiento

1. Pulse en **Buscar** en la barra de herramientas.
2. Identifique las características de la búsqueda y pulse en **Aceptar**.

#### Cómo buscar en un árbol de resultados:

##### Procedimiento

1. Pulse en **Buscar** en la barra de herramientas.
2. Identifique las características de la búsqueda y pulse en **Aceptar**.

#### Resultados

En una vista de resultados, puede buscar también en un subconjunto de los resultados visibles. Por ejemplo, puede querer buscar resultados en un subconjunto particular, como por ejemplo Tipo de vulnerabilidad.

## Vista Entradas y salidas

La vista Entradas y salidas proporciona la capacidad de visualizar resultados basados en un rastreo de entrada y salida.

La vista Entradas y salidas se divide en tres secciones:

- **Entradas y salidas:** En el panel izquierdo hay tres nodos de nivel superior:
  - **Entrada:** Un origen es una entrada para el programa, como un archivo, una solicitud de servlet, una entrada de consola o un socket. En la mayoría de los orígenes de entrada, los datos devueltos son ilimitados en términos de contenido y longitud. Cuando se deselecciona una entrada, se considera que está corrupta. Las entradas se enumeran en las tablas de resultados, en la columna **Entrada**.
  - **Salida:** Una salida puede tener cualquier formato externo en el que puedan escribirse datos. Como ejemplo de salida cabe citar las bases de datos, los archivos, la salida de la consola y los sockets. Escribir datos en una salida sin verificarla puede ser indicio de una grave vulnerabilidad de seguridad.
  - **Salida perdida:** Una salida perdida es un método de API del que no puede realizarse el rastreo.

Cada nodo se puede expandir para mostrar los paquetes afectados. Los paquetes, a su vez, pueden expandirse para mostrar las clases afectadas y a continuación los métodos. Estos métodos pueden expandirse para mostrar el paquete, clase y método que se encuentra al extremo opuesto del rastreo. Por ejemplo, si está preocupado por una salida en particular, puede incrementar el detalle hasta llegar al método bajo la raíz **Salidas**. Una vez allí, el árbol bajo ese método mostrará las vías de acceso hacia atrás a todas las entradas underneath that method would show the paths back to all of the sources que conducen a esa salida:

- Entradas
  - packageA
    - classA
      - methodA
    - packageB
      - classB
        - **methodB** (en el extremo opuesto del rastreo)
- Salidas
  - packageB
    - classB
      - **methodB**
        - packageA
          - classA
            - methodA
- Salidas perdidas

La selección hecha en esta vista de árbol determina qué se muestra en las otras dos secciones de la vista.

- **Nodos intermedios:** Esta sección de la vista muestra la unión de todos los nodos intermedios de los rastreos que se aplican a la selección hecha en la sección Entradas y salidas. Le permite refinar lo que se muestra en la tabla de resultados.

De manera predeterminada, esta sección está oculta. Puede mostrarse (o volver a ocultarse) pulsando en **Mostrar/Ocultar la tabla de llamadas intermedias**.

Para mostrar sólo los resultados de un paquete, clase o método, marque el recuadro de selección en la columna **Necesario** correspondiente. Para filtrar dejando fuera los resultados de un paquete, clase o método, marque el recuadro de selección en la columna **Eliminar** correspondiente. Los valores de filtro definidos en esta sección pueden utilizarse para crear un nuevo filtro.

**Ejemplo de uso:** Dado este nodo de árbol en la sección Entradas y salidas:

- Sources
  - java.util
  - Properties
  - getProperty

Cuando se selecciona `getProperty`, la tabla de resultados muestra solamente los resultados que contienen rastreos que tienen `getProperty` como entrada. En este punto, la sección de nodos intermedios mostrará todos los nodos intermedios (todos los nodos del rastreo excepto el de entrada y el de salida) para todos los rastreos que tengan una entrada de `getProperty`. Sin embargo, es posible que no le interese si el rastreo pasa por una API en particular. Por ejemplo, puede que tenga una rutina de validación que asegure que los datos procedentes de `getProperty` son válidos, y por lo tanto no desea ver los rastreos que pasan a través de esta rutina de validación. La sección de nodos intermedios incluirá esta rutina de validación, dado que es un nodo intermedio en el rastreo. Puede navegar hasta la rutina de validación en la sección de nodos intermedios y pulsar en el recuadro de selección **Eliminar**. Esto eliminará todos los resultados de la tabla que tengan rastreos que pasen a través de este nodo intermedio.

- **Resultados:** Esta sección contiene lo mismo que “Tabla Resultados” en la página 316 (y acciones asociadas) que “Vista Resultados” en la página 318 y otras vistas con resultados. Muestra los resultados de las entradas, salidas y nodos intermedios que ha elegido mostrar en las otras dos secciones de la vista.

---

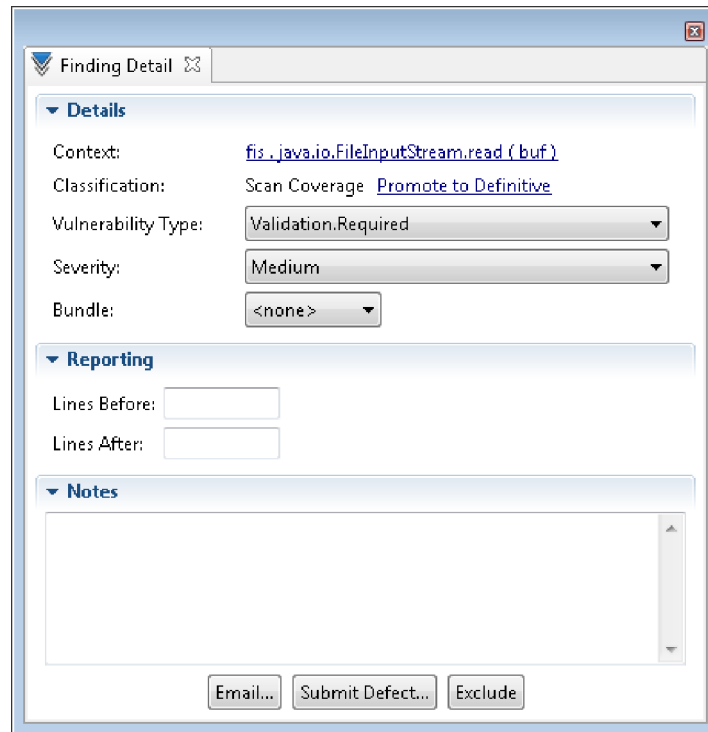
## Vistas que permiten investigar un resultado único

Las vistas en esta sección se utilizan para investigar resultados únicos.

- “Vista Detalle de resultado” en la página 178
- “Vista Asistencia de remediación” en la página 329
- “Vista Rastreo” en la página 329

### Vista Detalle de resultado

Al seleccionar un resultado, la vista Detalle de resultado muestra y le permite modificar sus propiedades. Con esta vista, puede modificar un resultado individual.



- “Sección Detalles” en la página 179
- “Sección Informes (sólo disponible en AppScan Source for Analysis y AppScan Source for Development (plugin de Eclipse))” en la página 179
- “Sección Notas” en la página 179
- “Acciones de la vista Detalles de resultados” en la página 179
- “Vista Detalles de resultados para resultados personalizados (disponible únicamente en AppScan Source for Analysis)” en la página 180

## Sección Detalles

- **Contexto:** fragmento de código que encierra la vulnerabilidad
- **Clasificación:** resultados de seguridad sospechosos o definitivos, o resultados de cobertura de escaneo, con un enlace para ascender el resultado a **Definitivo** o para volver al valor original si se cambió la clasificación.
- **Tipo de vulnerabilidad**
- **Gravedad:** alta, media, baja o informativa.
- **Paquete:** Nombre del paquete que contiene los resultados (no disponible en AppScan Source for Development (plugin de Visual Studio))

## Sección Informes (sólo disponible en AppScan Source for Analysis y AppScan Source for Development (plugin de Eclipse))

Especifique el número de líneas de código que deben incluirse en el informe antes o después del resultado.

## Sección Notas

Añadir notas al resultado.

## Acciones de la vista Detalles de resultados

- **Excluir:** Pulse en **Excluir** para excluir (eliminar) el resultado de la tabla de resultados. Para visualizar resultados excluidos, abra la vista Resultados excluidos.
- Sólo disponible en AppScan Source for Analysis:
  - **Correo electrónico:** Si ha configurado las preferencias del correo electrónico, puede enviar un resultado directamente a los desarrolladores para advertirles de potenciales defectos encontrados después de un escaneo. El correo electrónico incluye un archivo adjunto que contiene los resultados, y el texto del correo describe dichos resultados.
    1. Para enviar el resultado actual de la vista Detalle de resultado, pulse en **Correo electrónico**.
    2. En el cuadro de diálogo Nombre del archivo adjunto, especifique un nombre para el paquete de resultados que se adjuntará al correo electrónico. Por ejemplo, especificar `mi_resultado` en el campo **Nombre del archivo adjunto** hace que se adjunte al correo electrónico un paquete con el nombre de archivo `mi_resultado.ozbd1`.
    3. Pulse **Aceptar** para abrir el cuadro de diálogo Enviar resultados por correo electrónico. De forma predeterminada, el campo **Enviar a** del cuadro de diálogo Enviar resultados por correo electrónico se llenará con la **A dirección** que se especifica en las preferencias de correo electrónico. Sin embargo, se puede cambiar fácilmente al preparar el correo electrónico. En este cuadro de diálogo, revise el contenido del correo electrónico y pulse en **Aceptar** para enviar el correo electrónico.
  - **Enviar defecto:** Para enviar el resultado como defecto, pulse en **Enviar defecto**. De este modo se abrirá el cuadro de diálogo Seleccionar sistema de rastreo de defectos.
    - Si selecciona **ClearQuest** y pulsa en **Aceptar**, se abre el cuadro de diálogo Nombre del archivo adjunto. Especifique un nombre para el paquete de resultado que se adjuntará al defecto y pulse en **Aceptar**. Inicie una sesión en Rational ClearQuest y envíe los resultados.
    - Si selecciona **Quality Center** y pulsa **Aceptar**, se abre el cuadro de diálogo Inicio de sesión, que le permitirá iniciar la sesión en Quality Center para enviar los resultados.
    - Si selecciona la opción **Team Foundation Server**, se abre un recuadro de diálogo que le solicita que inicie la sesión en el sistema de seguimiento de defectos y proporcione otros detalles de configuración.

**Nota:** Rational Team Concert es el único sistema de seguimiento de defectos soportado en macOS.

## Vista Detalles de resultados para resultados personalizados (disponible únicamente en AppScan Source for Analysis)

La vista Detalle de resultado para resultados personalizados proporciona información adicional que puede editar:

- Archivo
- Línea
- Columna
- API



Además, el método mediante el cual puede editar los “Sección Detalles” en la página 179 es diferente del de los resultados estándar en algunos campos (por ejemplo, las clasificaciones para los resultados personalizados aparecen en una lista).

## Vista Asistencia de remediación

La Base de datos de conocimientos de AppScan Source Security proporciona inteligencia específica del contexto para cada vulnerabilidad. La base de datos de conocimientos indica el tipo de vulnerabilidad, por qué no es segura, cómo corregirla, y cómo evitarla en un futuro. Una vez que se ha escaneado el código fuente, la base de datos de conocimientos ofrece información específica necesaria para eliminar el riesgo de las aplicaciones de vital importancia. En la vista Asistencia de remediación aparece un aviso de remediación de la base de datos de conocimientos. Una vez que se ha realizado el escaneo, la base de datos de conocimientos ofrece información específica necesaria para eliminar el riesgo de las aplicaciones de vital importancia.

### Para ver la base de datos de conocimientos y obtener un aviso de remediación

- Seleccione un resultado en la tabla de resultados y, a continuación, abra la vista Ayuda o Asistencia de remediación de base de datos de conocimientos.
- En AppScan Source for Analysis, también puede seleccionar **Ayuda > Base de conocimientos de seguridad** en el menú para ver toda la base de datos de conocimientos.

Las API específicas de la base de datos enumeran el nivel y el tipo de gravedad. Por ejemplo, la API `strcpy()`, un tipo de desbordamiento de almacenamiento intermedio, tiene un nivel de gravedad alto. La descripción indica que `strcpy()` es susceptible de provocar un desbordamiento de la memoria de destino porque no conoce la longitud de la memoria de destino y por lo tanto no puede asegurarse de que no sobreescribe una zona vecina. Para corregir este problema, utilice `strncpy()`, que utiliza un parámetro de longitud.

Si el resultado tiene un ID de CWE (Common Weakness Enumeration) asociado, en la vista Asistencia de remediación, aparece un hipervínculo al tema CWE (CWE: <id>) en [http://cwe.mitre.org/data/definitions/<CWE\\_ID>.html](http://cwe.mitre.org/data/definitions/<CWE_ID>.html).

## Vista Rastreo

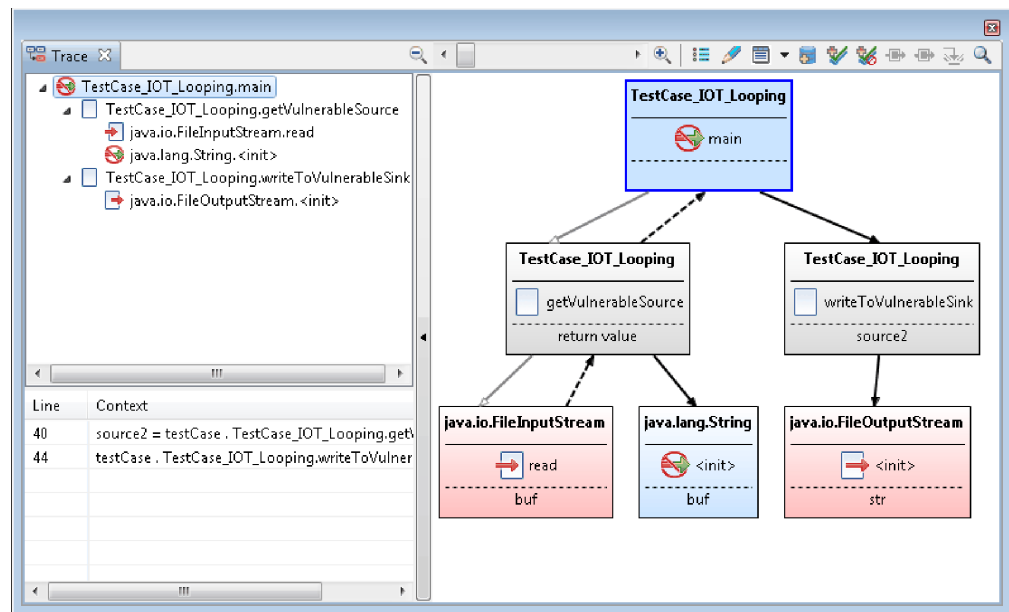
AppScan Source lleva a cabo análisis de entrada/salida e identifica y muestra estas vulnerabilidades. En la lista de resultados aparece un icono que identifica la fila que contiene una gráfica de rastreo de AppScan Source.

En la vista Rastreo puede ver el nodo raíz, donde confluyen las pilas de entrada y de salida. La pila de entrada es una serie de llamadas que conducen a una *entrada* de la que se sabe que suministra datos corruptos. La pila de salida es una serie de llamadas que conducen a una *salida*. Se genera un rastreo de AppScan Source cuando el código analizado puede rastrear el uso de una entrada no protegida hasta una salida no protegida.

- **Entrada:** Un origen es una entrada para el programa, como un archivo, una solicitud de servlet, una entrada de consola o un socket. En la mayoría de los orígenes de entrada, los datos devueltos son ilimitados en términos de contenido y longitud. Cuando se deselecta una entrada, se considera que está corrupta. Las entradas se enumeran en las tablas de resultados, en la columna **Entrada**.

- **Salida:** Una salida puede tener cualquier formato externo en el que puedan escribirse datos. Como ejemplo de salida cabe citar las bases de datos, los archivos, la salida de la consola y los sockets. Escribir datos en una salida sin verificarla puede ser indicio de una grave vulnerabilidad de seguridad.
- **Salida perdida:** Una salida perdida es un método de API del que no puede realizarse el rastreo.

Este diagrama ilustra la secuencia de llamada desde la raíz hasta la pila de entrada y la pila de salida.



En el diagrama:

- Las flechas huecas muestran una llamada que no tiene un flujo de datos corruptos conocido.
- Las flechas macizas tienen datos potencialmente corruptos. Las líneas de discontinuas muestran una vía de retorno.
- Las líneas Sólidas representan una llamada de método.

### Consejo:

- En la vista de rastreo, al mover el cursor sobre los nodos de rastreo en el gráfico, se proporciona información sobre el nodo.
- Los dos paneles de la izquierda en la vista (el panel de pilas de entrada/salida y el panel de flujo de datos) se pueden contraer para una mejor visualización del gráfico de llamadas gráficas. Seleccione el botón de flecha **Ocultar vista de árbol** para contraer estos paneles. Para visualizar estos paneles cuando están ocultos, seleccione el botón de flecha **Mostrar vista de árbol**.
- Mueva la barra de desplazamiento para acercarse y centrarse en los detalles, o para alejarse y tener una vista más amplia. Al pasar el ratón sobre la barra de desplazamiento de zoom se proporciona el nivel de zoom actual. Para llegar al nivel de máximo zoom, pulse **Zoom al 200%**. Para alejarse todo lo posible, pulse **Zoom para ajustar**.

## Vistas que permiten trabajar con asesoramientos

Las vistas en esta sección se utilizan para trabajar con asesoramientos a un nivel superior.

- “Vista Resumen de asesoramiento”
- “Vista Editor de filtros” en la página 332
- “Vista Matriz de vulnerabilidad” en la página 332

### Vista Resumen de asesoramiento

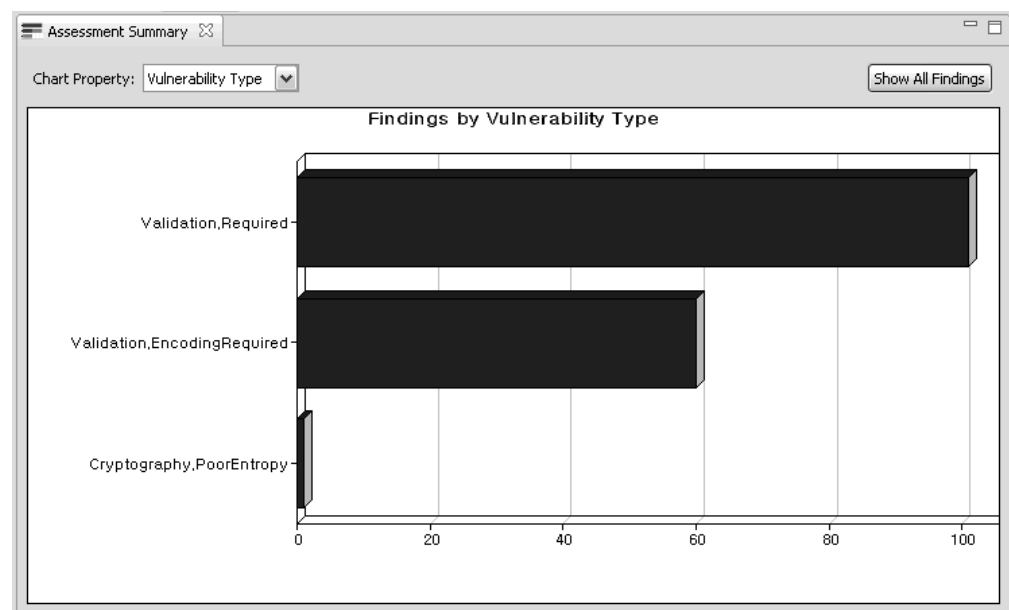
La vista Resumen de asesoramiento es una vista gráfica de diagrama de barras del asesoramiento abierto, y muestra información para los resultados seleccionados.

#### Nota:

- La vista Resumen de asesoramiento no está disponible en macOS.
- En AppScan Source for Development (plugin de Visual Studio), esta vista forma parte de la ventana Editar filtros.

Puede visualizar datos por una propiedad del diagrama:

- **Vulnerability Type:** Tipo de vulnerabilidad, como por ejemplo, `Validation.Encoding` o `Injection.SQL`
- **API:** Nombre de la API en la que se produce la vulnerabilidad.
- **Proyecto:** Resultados por proyecto si existe más de un proyecto.
- **Archivo:** Archivo individual en el que aparecen las vulnerabilidades.



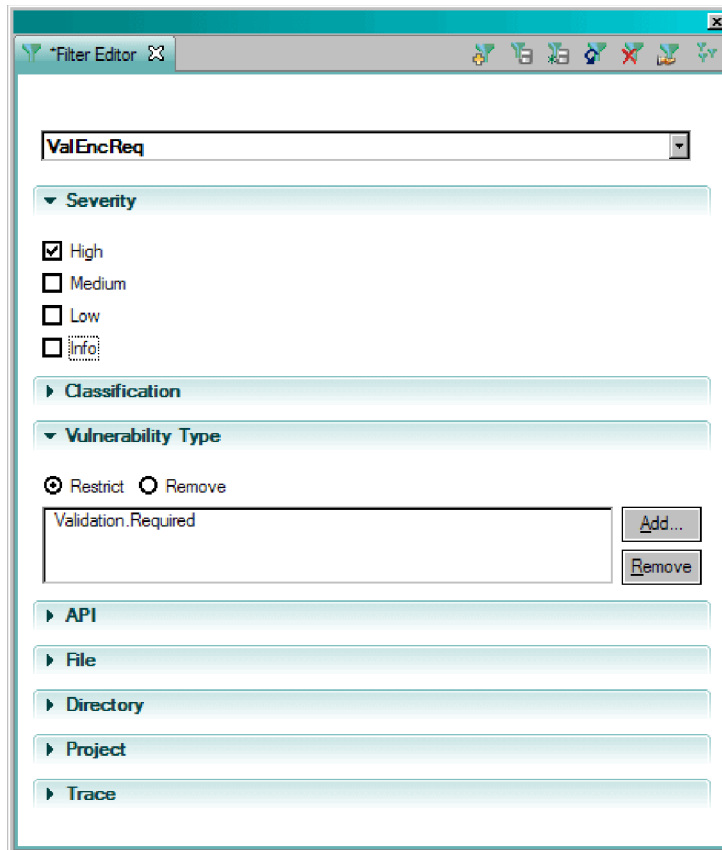
Pulse el diagrama para profundizar en los detalles de los resultados y empiece la selección.

**Consejo:** Si mueve el cursor sobre una barra de gráfico en la vista Resumen de asesoramiento proporciona el número exacto de resultados representados por la barra.

## Vista Editor de filtros

El Editor de filtros proporciona una manipulación más granular del filtro seleccionado actualmente que otras vistas de AppScan Source. Esta vista se compone de todos los criterios por los que se puede filtrar.

**Nota:** En AppScan Source for Development (plugin de Visual Studio), esta vista forma parte de la ventana Editar filtros.



**Consejo:** En la sección **Rastreo** de vista Editor de filtros, al mover el cursor sobre una entrada de rastreo, se proporcionan detalles acerca de la entrada.

## Vista Matriz de vulnerabilidad

La vista de la matriz de vulnerabilidad visualiza el número agregado de resultados de todas las aplicaciones incluidas en el escaneo. Las modificaciones a los resultados actualizan la matriz.

**Nota:** En AppScan Source for Development (plugin de Visual Studio), esta vista forma parte de la ventana Editar filtros.

| Reset  | Security Findings |         | Scan Coverage Findings | Totals |
|--------|-------------------|---------|------------------------|--------|
|        | Definitive        | Suspect |                        |        |
| High   | 0                 | 51      | 0                      | 51     |
| Medium | 0                 | 16      | 5                      | 21     |
| Low    | 0                 | 81      | 9                      | 90     |
| Totals | 0                 | 148     | 14                     | 162    |

Los resultados de seguridad y los resultados de cobertura de escaneo aparecen en recuadros coloreados que indican el orden de prioridad en que se deberían investigar o tratar dichos resultados:

1. Los resultados de seguridad definitivos de gravedad alta se resaltan en rojo, marcándolos con la prioridad más alta.
2. Los resultados de seguridad sospechosos de gravedad alta y los definitivos de gravedad media se resaltan en naranja y se deberían tratar a continuación.
3. Estas entradas de matriz se resaltan en amarillo, y se deberían considerar a continuación:
  - Resultados de seguridad definitivos de gravedad baja
  - Resultados de seguridad sospechosos de gravedad media y baja
4. Los resultados de cobertura de escaneo se representan con cuadrados grises y se les puede dar la prioridad más baja.

Cuando pulsa sobre una celda, cabecera de fila, o cabecera de columna de la **matriz de vulnerabilidad**, se actualiza el filtro actual para mostrar solamente los resultados en esa celda, fila o columna. Pulse en **Restablecer** para volver a una vista de todos los resultados.

En la vista Matriz de vulnerabilidad, los botones de la barra de herramientas controlan los números de los recuadros de color. Puede visualizar:

- Recuentos y totales de los resultados filtrados solamente
- Recuentos y número total de resultados

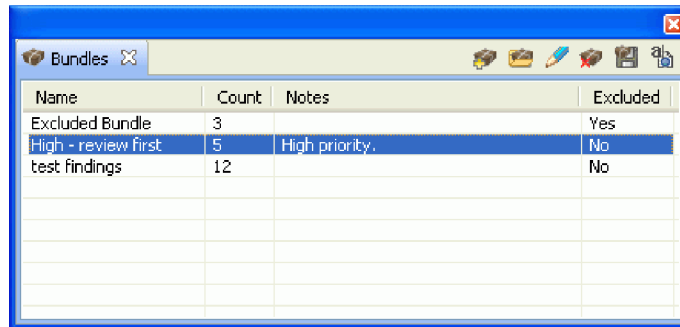
**Nota:** Los resultados de **Calidad** y los resultados clasificados con el nivel de gravedad **Info** no se incluyen en la vista Matriz de vulnerabilidad.

- Recuentos y número total de los resultados filtrados y de todos los resultados

**Nota:** Es posible que los filtros que se aplican fuera de la vista Matriz de vulnerabilidad no afecten a la vista Matriz de vulnerabilidad. El botón de la barra de herramientas **Mostrar recuentos de resultados filtrados** de la vista Matriz de vulnerabilidad se debe seleccionar para que el filtro refleje en la vista Matriz de vulnerabilidad.

## Vista Paquetes

En la vista Paquetes puede crear nuevos paquetes, añadir resultados a un paquete, ver paquetes y notas, renombrar o suprimir un paquete. Esta vista muestra el nombre del paquete, cualquier nota adjunta al paquete, el número de resultados del paquete y si el paquete está excluido. Cuando abre el paquete para ver su contenido, puede mover resultados a otros paquetes, modificar los resultados, editar el código o enviar el paquete a un sistema de seguimiento de defectos.



| Name                | Count | Notes          | Excluded |
|---------------------|-------|----------------|----------|
| Excluded Bundle     | 3     |                | Yes      |
| High - review first | 5     | High priority. | No       |
| test findings       | 12    |                | No       |
|                     |       |                |          |
|                     |       |                |          |
|                     |       |                |          |
|                     |       |                |          |

Para obtener más información, consulte “Selección con paquetes” en la página 172.

## Vista Paquetes

La vista Paquetes muestra los resultados en un paquete. Los paquetes son conjuntos de resultados creados en AppScan Source for Analysis.

Para ver los resultados en un paquete, efectúe una doble pulsación en un nombre de paquete en la vista Paquetes. El nombre de paquete aparece como título en la vista Paquetes. También puede importar un paquete y ver su contenido en la vista Paquetes. No puede modificar ni suprimir resultados de un paquete.

La vista Paquetes, similar a una tabla de resultados, contiene la siguiente información detallada:

Tabla 39. Columnas de la vista Paquetes

| Columna       | Descripción                                                                                                                                                                                                                                                                                                                                   |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rastreo       | Un icono en esta columna indica que existe un rastreo para salidas perdidas o conocidas.                                                                                                                                                                                                                                                      |
| Archivo       | Nombre del archivo de código donde se presenta el resultado de cobertura de escaneo o el resultado de seguridad. Las vías de acceso de archivos en los resultados son relativas al directorio de trabajo del proyecto escaneado.                                                                                                              |
| Clasificación | Tipo de resultado: resultado de seguridad <b>Definitivo</b> o <b>Sospechoso</b> o resultado de <b>Cobertura de escaneo</b> .<br><b>Nota:</b> En algunos casos, se puede utilizar una clasificación de <b>Ninguno</b> para denotar una clasificación que no corresponde a un resultado de seguridad ni a un resultado de cobertura de escaneo. |

Tabla 39. Columnas de la vista Paquetes (continuación)

| Columna                | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gravedad               | <ul style="list-style-type: none"> <li>• <b>Alta</b> : Supone un riesgo para la confidencialidad, integridad o disponibilidad de los datos o la integridad o disponibilidad de los recursos de proceso. A las condiciones de gravedad alta debe dárseles prioridad para su remediación inmediata.</li> <li>• <b>Media</b> : Supone un riesgo para la seguridad de los datos o la integridad de los recursos, pero la condición es menos susceptible de ser atacada. Las condiciones de seguridad media deben revisarse y resolverse cuando sea posible.</li> <li>• <b>Baja</b> : Supone un riesgo mínimo para la seguridad de los datos o la integridad de los recursos.</li> <li>• <b>Información</b> : El resultado, en sí mismo, no es susceptible de ser comprometido. Sino que describe las tecnologías, las características de la arquitectura o los mecanismos de seguridad utilizados en el código.</li> </ul> |
| Tipo de vulnerabilidad | Categoría de vulnerabilidad, como por ejemplo Validation.Required o Injection.SQL.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Contexto               | Fragmento de código que rodea la vulnerabilidad.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Método de llamada      | La función (o método) desde la que se realiza la llamada vulnerable.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| CWE                    | ID y tema del diccionario desarrollado por la comunidad que recoge las debilidades comunes del software (temas de CWE (Common Weakness Enumeration)).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Línea                  | Número de línea en el archivo de código que contiene la API vulnerable.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Notas                  | Notas que se hayan añadido a este resultado.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| ID de defecto          | ID de defecto en un sistema de seguimiento de defectos.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## Instalación y ubicaciones de archivo de datos de usuario

Al instalar AppScan Source, los datos de usuario y archivos de configuración se almacenan fuera del directorio de instalación.

- “Ubicación de instalación predeterminada” en la página 336
- “Directorio de datos AppScan Source predeterminado” en la página 336
- “Ubicación de archivos temporales de AppScan Source” en la página 336

## Ubicación de instalación predeterminada

Cuando AppScan Source esté instalado, el software se sitúa en una de estas ubicaciones predeterminadas:

- Versiones de 32 bits de Microsoft Windows:  
<SYSTEMDRIVE>:\Archivos de programa\IBM\AppScanSource
- Versiones de 64 bits de Microsoft Windows:  
<SYSTEMDRIVE>:\Program Files (x86)\IBM\AppScanSource
- Linux: Si es el usuario raíz, el asistente de instalación instala su software en /opt/ibm/appscansource. Si no es el usuario root, puede instalar el plugin AppScan Source for Development Eclipse, que se instala de forma predeterminada en <directorio\_inicial>/AppScan\_Source.
- macOS: /Applications/AppScanSource.app

### Importante:

- El nombre del directorio de instalación solo puede contener caracteres en inglés. Las carpetas que contengan caracteres que no sean del inglés no se permiten.
- Si está instalando en Windows, debe tener privilegios de administrador para poder instalar los componentes de AppScan Source.
- Si está instalando en Linux, debe tener privilegios raíz para poder instalar los componentes de servidor AppScan Source.

## Directorio de datos AppScan Source predeterminado

Los datos de AppScan Source constan de elementos como la configuración, muestra y archivos de registro. Cuando AppScan Source esté instalado, los archivos de datos se colocan en estas ubicaciones de forma predeterminada:

- Microsoft Windows: <SYSTEMDRIVE>:\ProgramData\IBM\AppScanSource

**Nota:** ProgramData\ es una carpeta oculta y para verla debe modificar las preferencias de vista en **Explorador** para visualizar los archivos y carpetas ocultos.

- Linux: /var/opt/ibm/appscansource
- macOS: /Users/Shared/AppScanSource

Para obtener información acerca de cómo cambiar la ubicación del directorio de datos de AppScan Source, consulte “Cómo cambiar el directorio de datos de AppScan Source” en la página 337.

## Ubicación de archivos temporales de AppScan Source

Algunas operaciones de AppScan Source dan lugar a la creación de archivos temporales, que se almacenan en estas ubicaciones de forma predeterminada:

- Microsoft Windows: <SYSTEMDRIVE>:\ProgramData\IBM\AppScanSource\temp

**Nota:** ProgramData\ es una carpeta oculta y para verla debe modificar las preferencias de vista en **Explorador** para visualizar los archivos y carpetas ocultos.

- Linux: /var/opt/ibm/appscansource/temp
- macOS: /Users/Shared/AppScanSource/temp



La ubicación de archivos temporales siempre se encuentra en un directorio temp en el directorio de datos AppScan Source. Puede cambiar la ubicación de archivos temporales cambiando el directorio de datos, como se describe en “Cómo cambiar el directorio de datos de AppScan Source”. Esto hará que temp se encuentre en el directorio de datos que ha seleccionado.

## Cómo cambiar el directorio de datos de AppScan Source

Es posible que desee cambiar la ubicación del directorio de datos de AppScan Source para gestionar el espacio de disco duro. Puede cambiar la ubicación después de la instalación de AppScan Source siguiendo los pasos del tema.

### Antes de empezar

Antes de completar la tarea, asegúrese de haber abandonado y cerrado todas las aplicaciones cliente de AppScan Source. Las aplicaciones cliente de AppScan Source son:

- AppScan Source for Analysis
- AppScan Source for Development (plugin de Eclipse o Visual Studio) (soportado solo en Windows y Linux)
- interfaz de línea de mandatos (CLI) de AppScan Source
- AppScan Source for Automation

Además, si ha instalado AppScan Source for Automation, asegúrese de haber cerrado servidor de automatización:

- En Windows, detenga el servicio **IBM Security AppScan Source Automation**.
- En Linux, emita este mandato: `/etc/init.d/ounceautod stop`
- En macOS, emita este mandato: `launchctl stop com.ibm.appscan.autod`

### Procedimiento

1. Defina una variable de entorno `APPSCAN_SOURCE_SHARED_DATA=<data_dir>`, donde `<data_dir>` es la ubicación en la que desea que se almacenen los datos de AppScan Source.

#### Nota:

- La ubicación `<data_dir>` debe ser una vía de acceso absoluta y completa que ya exista en la misma máquina que la instalación AppScan Source.
  - El nombre del directorio `<data_dir>` solo puede contener caracteres en inglés. Las carpetas que contengan caracteres que no sean del inglés no se permiten.
2. Localice el directorio de datos predeterminado que se ha creado cuando AppScan Source se ha instalado (consulte “Directorio de datos AppScan Source predeterminado” en la página 336 para aprender sobre las ubicaciones del directorio de datos predeterminado).
  3. Copie o mueva el contenido del directorio de datos predeterminado a la ubicación `<data_dir>` que se especifica en la variable de entorno.
  4. **Se aplica a AppScan Source for Automation instalado en Linux:**
    - a. Edite el archivo `/etc/init.d/ounceautod`.
    - b. Localice esta línea,

```
su - ounce -c
'export LD_LIBRARY_PATH="/opt/IBM/AppScan_Source/bin":$LD_LIBRARY_PATH &&
cd "/opt/IBM/AppScan_Source/bin" &&
"/opt/IBM/AppScan_Source/bin/ounceautod" -s' >>
"/var/opt/ibm/appscansource/logs/ounceautod_output.log" 2>&1 &
```

y sustitúyela por:

```
su - ounce -c
'export APPSCAN_SOURCE_SHARED_DATA=<new data directory path here> &&
export LD_LIBRARY_PATH="/opt/IBM/AppScan_Source/bin":$LD_LIBRARY_PATH &&
cd "/opt/IBM/AppScan_Source/bin" &&
"/opt/IBM/AppScan_Source/bin/ounceautod" -s' >>
"<vía_acceso_nuevo_directorio_datos>/logs/ounceautod_output.log" 2>&1 &
```

**Nota:** El mandato anterior es una línea.

c. Guarde el archivo /etc/init.d/ounceautod.

## Qué hacer a continuación

Si ha instalado AppScan Source for Automation, inicie el servidor de automatización:

- En Windows, inicie el servicio **IBM Security AppScan Source Automation**.
- En Linux, ejecute este mandato: /etc/init.d/ounceautod start
- En macOS, emita este mandato: launchctl start com.ibm.appscan.autod

---

## Capítulo 15. Soporte a CWE

CWE (Common Weakness Enumeration) es una lista estándar del sector que proporciona nombres comunes para debilidades de software conocidas de forma pública. En este tema se proporciona una lista de ID de CWE a los que la versión actual de AppScan Source da soporte.

Durante los escaneos, AppScan Source busca estos identificadores de la lista de CWE y sus identificadores padre o hijo:

*Tabla 40. Soporte a CWE*

|                                                                                               |
|-----------------------------------------------------------------------------------------------|
| 15, 16, 20, 73, 74, 77, 79, 88, 89, 90, 91, 95, 98                                            |
| 105, 109, 112, 113, 116, 117, 120, 129, 130, 131, 134, 185, 190                               |
| 201, 209, 242, 250, 257, 264, 266, 267, 285, 287, 288, 295                                    |
| 310, 311, 312, 319, 327, 331, 335, 345, 352, 359, 367, 382, 388, 390, 398                     |
| 400, 404, 407, 425, 434, 447, 470, 472, 477, 489, 497                                         |
| 506, 507, 511, 517, 520, 521, 522, 523, 524, 525, 532, 538, 543, 544, 546, 547, 565, 569, 586 |
| 601, 613, 615, 624, 643, 645                                                                  |



---

## Glosario

Este glosario incluye términos y definiciones para AppScan Source.

En este glosario se utilizan las siguientes referencias cruzadas:

- Consulte le lleva de un término a un sinónimo preferido o de un acrónimo o abreviatura al formato completo definido.
- Consulte también le remite a un término relacionado o a uno opuesto.

Para ver glosarios de otros productos de IBM, vaya a [www.ibm.com/software/globalization/terminology](http://www.ibm.com/software/globalization/terminology).

---

### A

#### **aplicación**

Uno o varios programas informáticos o componentes de software que ofrecen una función que proporciona soporte directo de uno o varios procesos comerciales específicos.

#### **asesoramiento**

Grupo de resultados del escaneo de un código con el que el usuario puede trabajar y que puede guardar y compartir con otras personas.

#### **ataque**

Intento, por parte de una persona no autorizada, de comprometer el funcionamiento de un programa de software o sistema en red.

#### **atributo**

Característica de una aplicación que ayuda a organizar los resultados de un escaneo en grupos significativos, como por ejemplo por departamento o por gestor de proyecto.

---

### C

#### **codificar**

En seguridad de sistemas, convertir texto llano a un formato ininteligible mediante un sistema de códigos.

#### **conjunto**

Agrupación de tipos y recursos que forman una unidad de despliegue, control de versión, reutilización, ámbito de activación y permisos de seguridad en aplicaciones de .NET Framework.

#### **corrupto**

Datos no seguros cuyo flujo por el código se permite.

---

### D

#### **defecto**

Tipo de solicitud de cambio que identifica una anomalía o fallo en un producto de trabajo.

#### **Densidad-V**

Expresión numérica que proporciona una forma coherente de evaluar la vulnerabilidad de sus aplicaciones. La densidad-V se calcula relacionando

el número e importancia crítica de las vulnerabilidades y excepciones con el tamaño de la aplicación o proyecto que se analiza.

**devolución de llamada**

Método con el que una hebra notifica a una hebra de otra aplicación que se ha producido un suceso.

---

## E

**escaneo**

El proceso por el que AppScan explora y prueba una aplicación y proporciona resultados.

**espacio de trabajo**

Interfaz de usuario y entorno de desarrollo integrado (IDE) de las herramientas de Eclipse y basadas en Eclipse, como por ejemplo IBM Rational Application Developer.

**excepción**

Indicación de una condición sospechosa y potencialmente vulnerable que requiere información o investigación adicionales.

**exclusión**

Resultado que un usuario puede marcar y pasar por alto.

---

## F

**filtro** Conjunto de reglas que definen resultados con ciertos rasgos.

---

## G

**gráfico de llamadas**

Gráfico que utiliza líneas que representan el flujo de datos entre las subrutinas de un programa.

---

## M

**memoria caché de análisis de vulnerabilidad**

Memoria caché de vulnerabilidades halladas durante un escaneo de código fuente que se puede utilizar en futuros escaneos para reducir el tiempo de escaneo.

---

## P

**paquete**

Conjunto de resultados que crea el usuario. Los paquetes se pueden exportar y compartir entre personas y aplicaciones.

**perspectiva**

Grupo de vistas que muestran diversos aspectos de los recursos del espacio de trabajo.

**pila**

Área de la memoria que suele almacenar información de tipo información sobre registros temporales, valores de parámetros y direcciones de devolución de subrutinas y que se basa en el principio de último en entrar, primero en salir (LIFO).

---

## R

### **regla de patrón**

Patrón o expresión regular que se busca durante un escaneo.

### **Remediación**

Sugerencia de cómo solucionar un problema.

### **resultado**

Descubrimiento de una instancia de un riesgo de seguridad en un código. AppScan divide los resultados en dos categorías: vulnerabilidades y excepciones.

---

## S

### **salida perdida**

Método de API del que ya no puede realizarse el rastreo.

### **scripts entre sitios**

Técnica de ataque que obliga a un sitio web a duplicar datos suministrados por el cliente, que se ejecutan en el navegador web de un usuario.

### **selección**

Proceso de evaluar resultados y determinar cómo resolverlos.

### **sink**

Cualquier formato externo en el que puedan escribirse datos. Como ejemplo de salida cabe citar las bases de datos, los archivos, la salida de la consola y los sockets.

**socket** Descriptor de contexto de comunicaciones que utiliza TCP/IP.

---

## X

**XSS** Consulte scripts entre sitios.





---

## Avisos

Esta información se ha desarrollado para productos y servicios ofrecidos en los Estados Unidos. Es posible que en otros países IBM no ofrezca los productos, servicios o características que se describen en este documento. Solicite información al representante local de IBM acerca de los productos y servicios disponibles actualmente en su zona. Las referencias a programas, productos o servicios de IBM no pretenden establecer ni implicar que sólo puedan utilizarse dichos productos, programas o servicios de IBM. En su lugar, se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no infrinja los derechos de propiedad intelectual de IBM. No obstante, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o aplicaciones pendientes de patente que cubran los temas descritos en este documento. La posesión de este documento no otorga ninguna licencia sobre dichas patentes. Puede enviar las consultas sobre licencias, por escrito, a la siguiente dirección:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785, EE. UU.

Si tiene alguna pregunta sobre la licencia relacionada con la información del juego de caracteres de doble byte (DBCS), póngase en contacto con el departamento de propiedad intelectual de IBM de su país o envíe sus preguntas por escrito a:

Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan, Ltd.  
19-21, Nihonbashi-Hakozakicho, Chuo-ku  
Tokio 103-8510, Japón

**El párrafo siguiente no se aplica al Reino Unido ni a ningún otro país donde estas disposiciones sean incompatibles con la legislación vigente:**

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍA DE NINGÚN TIPO, YA SEA EXPLÍCITA O IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN, COMERCIALIZACIÓN O IDONEIDAD PARA UNA FINALIDAD DETERMINADA.

Algunos países no permiten la renuncia a garantías expresas o implícitas en ciertas transacciones, por lo que el párrafo anterior puede no aplicarse en su caso.

Esta información puede contener imprecisiones técnicas o errores tipográficos. Periódicamente, se efectúan cambios en la información incluida en este documento; estos cambios se incorporarán en nuevas ediciones de la publicación. IBM puede realizar mejoras y/o modificaciones en los productos y/o programas descritos en esta publicación en cualquier momento sin aviso.

Las referencias en esta información a sitios web que no son de IBM se proporcionan solo por conveniencia y bajo ningún concepto se considerarán un anexo a esos sitios web. La información contenida en dichos sitios web no forma parte de la información del presente producto de IBM y el cliente es responsable de la utilización de dichos sitios web.

IBM puede utilizar o distribuir la información que se le proporcione del modo que considere adecuado sin incurrir por ello en ninguna obligación con el remitente.

Los licenciarios de este programa que deseen obtener información acerca del mismo con el fin de: (i) intercambiar la información entre los programas creados independientemente y otros programas (incluido éste) y (ii) utilizar mutuamente la información que se ha intercambiado, deben ponerse en contacto con:

IBM Corporation  
2Z4A/101  
11400 Burnet Road Austin, TX 78758 EE.UU.

Dicha información puede estar disponible, sujeta a los términos y condiciones adecuados, incluido en algunos casos el pago de una tarifa.

IBM proporciona el programa bajo licencia que se describe en este documento y todo el material bajo licencia disponible para éste en función de los términos del IBM Customer Agreement, IBM International Program License Agreement o cualquier otro acuerdo equivalente entre ambas partes.

Los datos de rendimiento incluidos aquí se determinaron en un entorno controlado. Por lo tanto, los resultados que se obtengan en otros entornos operativos pueden variar significativamente. Pueden haberse realizado algunas mediciones en sistemas a nivel de desarrollo y no existe ninguna garantía de que estas mediciones vayan a ser equivalentes en sistemas disponibles generalmente. Además, puede que algunas medidas se hayan estimado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables a su entorno específico.

La información concerniente a productos no IBM se ha obtenido de los suministradores de dichos productos, de sus anuncios publicados o de otras fuentes de información pública disponibles. IBM no ha probado esos productos y no puede confirmar la precisión del rendimiento, la compatibilidad ni ninguna otra afirmación relacionada con productos que no son de IBM. Las consultas acerca de las posibilidades de los productos no IBM deben dirigirse a los suministradores de los mismos.

Todas las declaraciones relativas a la dirección o a la intención futura de IBM están sujetas a cambios o anulación sin previo aviso y representan únicamente metas y objetivos.

Todos los precios de IBM que se indican son precios de venta al público sugeridos de IBM, son actuales y están sujetos a cambio sin previo aviso. Los precios de cada comercio específico pueden variar.

Esta información sólo es para fines de planificación. La información está sujeta a cambios antes de que los productos aquí descritos estén disponibles.

Esta información contiene ejemplos de datos e informes utilizados en operaciones comerciales diarias. Para ilustrarlas de la manera más completa posible, los

ejemplos incluyen nombres de individuos, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier parecido con los nombres y direcciones utilizados por una empresa real es mera coincidencia.

#### LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de ejemplo en lenguaje fuente, que se utilizan para complementar las explicaciones relacionadas con las técnicas de programación en diversas plataformas operativas. Puede copiar, modificar y distribuir estos programas de ejemplo en cualquier formato sin abonar ninguna cantidad a IBM, con la finalidad de desarrollar, utilizar, comercializar o distribuir programas de aplicación conformes a la interfaz de programación de aplicación para la plataforma operativa para la cual se han escrito los programas de ejemplo. Los ejemplos no se han probado minuciosamente bajo todas las condiciones. Por lo tanto, IBM no puede asegurar ni implicar la fiabilidad, utilidad o función de estos programas. Puede copiar, modificar y distribuir dichos programas de ejemplo en cualquier formato y sin tener que abonar una cuota a IBM, a fin de desarrollar, utilizar, comercializar o distribuir programas de aplicación que se adapten a las interfaces de programación de aplicaciones de IBM.

Cada copia o cada parte de los programas de ejemplo o de los trabajos que se deriven de ellos debe incluir un aviso de copyright como se indica a continuación:

© (nombre de la empresa) (año). Algunas partes de este código se derivan de programas de ejemplo de IBM Corp. © Copyright IBM Corp. \_escriba el año o los años\_. Reservados todos los derechos.

Si está consultando esta información en copia software, es posible que no se vean las fotografías y las ilustraciones de color.

### **Marcas registradas**

IBM, el logotipo de IBM, e [ibm.com](http://ibm.com) son marcas o marcas registradas de International Business Machines Corp., registradas en muchas jurisdicciones de todo el mundo. Otros productos y nombres del servicio pueden ser marcas registradas de IBM u otras compañías. Encontrará una lista actual de marcas registradas de IBM en la página web Copyright and trademark information situada en [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Adobe, Acrobat, PostScript y todas las marcas comerciales basadas en Adobe son marcas registradas de Adobe Systems Incorporated en Estados Unidos o en otros países.

IT Infrastructure Library es una marca registrada de Central Computer and Telecommunications Agency, que forma parte de Office of Government Commerce.

Intel, el logotipo de Intel, Intel Inside, el logotipo de Intel Inside, Intel Centrino, el logotipo de Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium y Pentium son marcas registradas de Intel Corporation o de alguna de sus empresas subsidiarias en los Estados Unidos de América y en otros países.

Linux es una marca registrada de Linus Torvalds en Estados Unidos o en otros países.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en Estados Unidos o en otros países.

ITIL es una marca registrada y una marca comunitaria registrada de OGC (Office of Government Commerce), registrada en la Oficina de Patentes y Marcas de Estados Unidos.

UNIX es una marca comercial registrada de The Open Group en los Estados Unidos y otros países.

Java y todas las marcas comerciales basadas en Java son marcas comerciales o marcas registradas de Oracle y/o sus filiales.

Cell Broadband Engine es una marca registrada de Sony Computer Entertainment, Inc en los Estados Unidos y/o en otros países y se utiliza bajo licencia.

Linear Tape-Open, LTO, el logotipo de LTO, Ultrium y el logotipo de Ultrium son marcas registradas de HP, IBM Corp. y Quantum en EE.UU. y en otros países.

# Índice

## Caracteres Especiales

.dsp 49  
.ewf 36  
.jsp 64  
.jspx 64  
.ozasmt 139  
.ozbdl 175, 221  
.paf 37  
.sln 36  
.vcproj 49  
.war 58, 259, 299

## A

abrir proyecto de Web Application Security 225  
ámbito 198  
    Específicas de API 198  
    específico de sitio de llamada 198  
ámbito específico de API 198  
ámbito específico de sitio de llamada 198  
análisis basado en patrón 67  
análisis de entrada/salida 329  
añadir un nuevo proyecto 51, 52  
API Java  
    requisito de sintaxis 247  
aplicación  
    abrir 37  
    añadir existente 41  
        acciones de la interfaz de usuario 42  
        arrastrar y soltar 42  
    añadir varios 43  
        acciones de la interfaz de usuario 43  
        arrastrar y soltar 43  
    crear nueva 37  
    definido 20  
    eliminar 85  
    Importar desde un servidor de aplicaciones 44  
        ampliar la infraestructura de importación del servidor de aplicaciones 267  
        generar JSP precompilado para Liberty Profile 45  
aplicar filtro 168  
aplicar filtro de forma global 168  
Application Discovery Assistant 38  
    reglas de exclusión predeterminadas 41  
AppScan Enterprise Server  
    certificado SSL 26  
    modificar contraseña 26  
AppScan Source  
    familia de productos 1  
    for Analysis 1, 19, 111

AppScan Source (*continuación*)  
    conceptos 20  
    for Automation 1  
    for Development 1  
    Inicio de sesión de AppScan Enterprise Server 22  
        CAC 24  
        certificado SSL 26  
        modificar contraseña 26  
    problemas de accesibilidad 27  
archivo WAR 64, 187, 197  
archivos de AppScan Source  
    epf 33  
    ewf 33  
    gaf 33  
    gpf 33  
    paf 33  
    ppf 33  
archivos de clase Java 58  
    precompilado 58  
archivos de clase Java precompilados 58  
archivos JAR 64  
asesoramiento 20, 109  
    análisis en la nube 127  
    comparar 148, 315  
    guardado 109  
    publicado 109, 132  
asesoramientos  
    comparar en vista Diferencia entre asesoramientos 182  
    comparar entre la vista Mis asesoramientos o Asesoramientos publicados 182  
    eliminación 141  
    guardar 139  
    guardar automáticamente 140  
    publicación 132  
Asistente de configuración de nueva aplicación 36  
Asistente de reglas personalizadas 240  
atributos 258, 259, 296, 297, 299  
    aplicación 84, 258, 259, 297, 299  
    creación 299  
    definido 20  
    global 84, 258, 259, 297, 299  
atributos de aplicación 84  
atributos globales 84, 297  
ayuda en línea 285  
ayuda flotante 286

## B

barra de estado 287  
barra de herramientas 286  
base de datos de conocimientos 1, 285, 329  
Base de datos de conocimientos de AppScan Source Security 1, 239, 329

## C

cancelar escaneo 125  
Carga automática de campos de errores 101, 212  
Categorías 231, 308  
clasificación 146, 151, 242  
    cobertura de escaneo 21  
    definitivo 21  
    sospechoso 21  
codificación 192  
Common Weakness Enumeration 146, 223  
comparar asesoramientos 148, 315  
compilación de JSP 97  
compilador  
    JSP 106  
    Tomcat 106  
    WebLogic 106  
    WebSphere Application Server 106  
condiciones de regla  
    Confianza 151  
    Gravedad 151  
    Tipo 151  
configuración 33  
    aplicaciones 36  
    proyectos 47  
Configuración 275  
configuración de servidor de correo de SMTP 106  
conjuntos de reglas de patrón  
    aplicación 254  
    creación en la vista Biblioteca de reglas de escaneo 249  
    eliminación 249  
    modificar 249  
consola  
    error 312  
    salida 312  
consola de errores 312  
consola de salida 312  
copiar un proyecto 277  
creación de paquetes 173  
    en la vista Paquetes 173  
    en la vista Resultados 173  
crear filtro 162  
    desde la vista Resumen de asesoramiento 164  
    editor de filtros 163  
    Vista Entradas y salidas 167  
crear informe personalizado 226  
CWE 146, 223, 318, 323, 329

## D

definición de variables  
    cuando se publica y se guarda 142  
    ejemplo 142  
definitiva 242  
Densidad-V 242, 247, 313

- dependencias del proyecto 58, 69, 259, 299
- dependencias del proyecto Java 58
- dependencias del proyecto JSP 58
- devolución de llamada corrupta 240
- Diferencia entre asesoramientos 148, 182
- directorio de instalación
  - predeterminado 126, 335
- directorio WEB-INF 58, 64, 259, 299
- DISA Application Security and Development 225, 228
- Diseño de informe 231, 308
  - Editor de informe 231, 232, 308, 309

## E

- Eclipse 187, 197
- editor
  - externo 283
  - interno 283
- Editor de informe 231, 308
  - categorías 231, 308
  - Diseño 232, 309
  - Separador Categorías 234, 310
  - separador Vista previa 235, 312
  - Vista previa 231, 308
- editor externo 187, 197, 283
  - Eclipse 187, 197
  - Notepad 187, 197
  - vi 187, 197
  - Visual Studio.NET 187, 197
- editor interno 187, 197, 283
- egrep 251
- ejecutable de CQPerl 217
- ejemplos de código 201
  - ejemplo 1: desde origen a receptor 201
  - ejemplo 2: creación de una rutina de validación/codificación
    - desde el Asistente de reglas personalizadas 207
    - desde la vista Rastreo 204
  - ejemplo 2: modificación entre origen y receptor 203
  - ejemplo 3: distintos archivos de origen y de recepción 208
  - ejemplo 4: validación en profundidad 209
- eliminación de asesoramientos 141
- eliminar regla 151
- entorno de trabajo 275
- escaneo 109
  - configuraciones de escaneo 113
  - incremental 122
- escaneo basado en patrón 258, 259, 297, 299
- espacio de trabajo 275
  - añadir 46
- estructura de archivos JSP 64
- exclusión de archivos de escaneos 124
- exclusiones 148, 169, 258, 259, 296, 297, 299, 321
  - aplicación 169
  - especificación 170
  - especificación de filtro 171
    - ejemplo 1 171
    - ejemplo 2 172

- exclusiones (*continuación*)
  - filtro 169
  - global 169
  - marcar resultados como en tabla de resultados 170, 171
  - paquete 169, 172
  - proyecto 169
- exclusiones de aplicación 169
- exclusiones de proyecto 169
- exclusiones globales 169
- expresiones include de PHP no resueltas 71, 76
- expresiones regulares 247, 248, 250, 251
  - egrep 251
  - grep 250
  - Perl 250
- extensión de archivo de proyecto 107

## F

- fallos
  - resolución 186
- filtrar exclusiones 169
- filtro 148
  - aplicar 168
    - globalmente 168
  - compartido 148, 163
  - crear 162
    - desde la vista Resumen de asesoramiento 164
    - en la vista Editor de filtros 163
    - en la vista Entradas y salidas 167
  - definido 151
  - desde matriz de vulnerabilidad 166
  - determinar 169
  - local 148
  - predefinido 156
  - predefinido archivado 159
    - acceso 161
  - publicación 134
  - tipos de vulnerabilidades 151
- filtro compartido 148, 163
- filtro local 148
- FIPS 2
- FIPS (Federal Information Processing Standard) 2
- flujo de datos 195
- flujo de trabajo 19
- fragmento de código 223

## G

- Gestión de la base de datos de conocimientos 239
  - permisos 239
- gestión de usuarios 284
- glosario 341
- gráfico de llamadas 195
- Gráfico de sentencias JavaScript 196
- gravedad 146, 242
- grep 247, 248, 250
- guardar asesoramiento 109
- guardar asesoramientos 139
  - automáticamente 140

## H

- hiperenlaces de ID de CWE 223
- HP Quality Center 100, 211, 216
  - envío de resultados a 216
  - información de resultados 217
  - seguimiento de resultados 216

## I

- IBM Rational ClearQuest 217
  - envío de defectos 218
- información de depuración 58
- informativo 240
- Informe de AppScan Source 225
- Informe de CWE/SANS Top 25 2011 227
- informe de Payment Card Industry Security Standard 223, 225
- informe de PCI 223
- informe de PCI Data Security Standard Versión 3.0 228
- Informe OWASP Top 10 2013 228
- informe personalizado
  - inclusión de categorías
    - adición de paquetes 236
- informes
  - Informe de AppScan Source 223
  - Perfil 223
  - Resultados 223
- informes de resultados 223
- informes personalizados 231
  - diseño 236
  - generación 235
  - guardar plantillas 237
  - inclusión de categorías 236
    - adición de propiedades 237
    - adición de resultados 237
  - vista previa 237
- instalación
  - importador de Application Developer 47
  - importador de Eclipse 47
  - ubicación de archivo 126, 335
  - ubicación de datos 126, 335
    - modificación 337
- Integración de AppScan Enterprise Console 135
- IPv6 2

## J

- Java Development Kit 106, 281
- JavaServer Pages 281
- JDK 58, 106, 259, 281, 299
  - predeterminado 58, 106
- JDK predeterminado 106
- JSP 281
  - compilador 106

## M

- matriz de vulnerabilidad 166, 332
- menú
  - Administración 284
  - Archivo 277

menú (*continuación*)

- Editar 281
- Escanear 282
- Herramientas 283
- Perspectiva 284
- principal 277
- Vista 284

menú Administración 284

menú Archivo 277

menú Editar 281

menú Escanear 282

menú Herramientas 283

menú Perspectiva 284

menú principal 277

menú Vista 284

Microsoft Visual Studio 36

Migración 15

muestra 273

## N

NIST 2

NIST (National Institute of Standards and Technology) 2

Notepad 187, 197

Novedades 4

## O

orden de clasificación 146

- clasificación 146

- gravedad 146

Ounce/Ant 33, 49

Ounce/Make 33, 49

OWASP 225

OWASP Mobile Top 10 228

## P

paquetes 20, 148, 172, 258, 297

- adición de resultados a 174

- asignación 176, 221

- creación 173

  - en la vista Paquetes 173

  - en la vista Resultados 173

- excluidos 169, 172, 258, 297

- guardar 175

- mover resultados entre 174

- resultados en 175

- resultados solucionados/que

  - faltan 175

- visualización de resultados en 175

patrones 247, 248, 258, 259, 297, 299

- búsqueda de texto 251

patrones de texto

- definición 251

PBSA 67

Perl 250, 251

perspectiva Análisis 275

perspectiva Configuración 275

perspectiva Selección 275

perspectivas 275

- Análisis 275

- Selección 275

Plugin Ounce/Maven 33

preferencias 93, 281

preferencias (*continuación*)

- AppScan Enterprise Console 96, 138

- Artículos de la base de datos de

  - conocimientos 107

- correo electrónico 106

- extensión de archivo de proyecto 107

- General 93

- HP Quality Center 101, 212

  - personalizar campos 103, 214

- importador de Eclipse 48, 105

- Java 106

- JavaServer Page 106

- JSP 106

- Rational ClearQuest 100, 211

- Rational Team Concert 103, 215

  - renombrar servidor 104

- servidor de aplicaciones 97

- sistema de seguimiento de

  - defectos 100, 211

  - HP Quality Center 101, 212

  - Rational ClearQuest 100, 211

  - Rational Team Concert 103, 104,

    - 215

  - renombrar servidor 104

  - Team Foundation Server 104, 215

- Team Foundation Server 104, 215

- Tomcat 7 97

- WebLogic 11 98

- WebLogic 12 98

- WebSphere 98

productos 1

Productos de AppScan Source 1

propagadores corruptos 240

propiedades

- archivo 305

propiedades de archivo 305

Protocolo de Internet versión 6 2

proyecto

- eliminar 85

proyecto de JavaScript 66

proyectos

- .NET Assembly

  - añadir 67

- análisis de patrón

  - añadir 67

- añadir a aplicación 49

- añadir existente 49

  - acciones de la interfaz de

  - usuario 50

- arrastrar y soltar 50

- añadir varios 51

  - acciones de la interfaz de

  - usuario 51

- arrastrar y soltar 52

- Arxan

  - añadir 53

- ASP

  - añadir 54

- ASP clásico 49

- C/C++ 49

  - añadir 55

- COBOL

  - añadir 57

- ColdFusion

  - añadir 57

- copia 83

- definido 20

proyectos (*continuación*)

- Java 49

  - añadir 58

- JavaScript

  - añadir 66

- JSP 49

  - añadir contenido 64

- modificar 83

- Perl

  - añadir 68

- PHP

  - añadir 69

- PL/SQL

  - añadir 80

- T-SQL

  - añadir 81

- Visual Basic 49

  - añadir 82

proyectos .NET Assembly 67

proyectos Arxan 53

proyectos ASP 54

proyectos COBOL 57

proyectos ColdFusion 57

proyectos JSP 64

proyectos Perl 68

proyectos PL/SQL 80

proyectos T-SQL 81

publicación de asesoramientos 132

publicar asesoramientos 109, 132, 277

- AppScan Enterprise Console 135

- AppScan Source 133

  - suprimir 134

## Q

Quality Center 216

- envío de resultados a 216

- información de resultados 217

- seguimiento de resultados 216

## R

RAD 47

raíz de contenido ASP 54

raíz de contexto web 58, 64, 259, 299

raíz de documento PHP 69

raíz de origen 58, 69

rastreo 191, 247

- búsqueda 193

- resultados de escaneo 192

rastreo de AppScan Source 191, 323

rastreo de entrada/salida 193

Rational Application Developer for

- WebSphere Software (RAD) 47

Rational ClearQuest 100, 211

- envío de resultados 217

- guardar defectos 221

Rational Team Concert 100, 211, 218

- certificados SSL 104, 219

- envío de defectos 219

registro automático 132

registro de errores 285

regla

- eliminar 151

- restringir para 151

regla de ausencia 251

- reglas de patrón 239, 247, 248
  - aplicación 254
  - creación en la vista Biblioteca de reglas de patrón 251
  - definición 250
  - eliminación 253
  - modificar 253
- reglas personalizadas
  - atributo de probabilidad 246
  - devolución de llamada corrupta 240
  - informativo 240
  - no susceptible a corrupción 240
  - propagadores corruptos 240
  - resultado de no rastreo 240
  - rutina de validación/codificación 240
  - sink 240
  - source 240
- restringir para regla 151
- resultado perdido 321
- resultados
  - anotación en la vista Paquetes 176
  - ascender clasificación 177
  - ausentes 284, 313
  - buscar 323
    - en una tabla de resultados 324
    - todas las apariciones de un elemento 323
  - clasificación 21
  - comparación 182
  - comparación en el menú principal 182
  - comparación en vista Diferencia entre asesoramientos 182
  - común 182
  - eliminar modificaciones 180
  - excluidos 258, 284, 297
  - modificar gravedad 177
  - modificación desde una tabla de resultados 177
    - cambiar vulnerabilidad 177
  - modificación desde una Tabla de resultados
    - anotación 178
    - ascender clasificación 177
    - modificar gravedad 177
  - modificado 148, 258, 284, 297
  - modificar 176
  - modificar en la vista Detalle de resultado 178
  - nuevo 182
  - personalizado 183, 258, 297
    - creación en el Editor de código fuente 185
    - creación en la página Propiedades 184
    - creación en una vista de resultados 185
    - eliminación en la página Propiedades 185
    - modificación en la página Propiedades 185
  - solucionados/que faltan 182
    - personalizado 183
  - tabla 187, 197
  - visualización 146
- resultados ausentes 284
- resultados de la búsqueda 193, 324

- resultados excluidos 258, 284, 297
- resultados modificados 148, 258, 284, 297
- resultados personalizados 183, 258, 297
  - creación en el Editor de código fuente 185
  - creación en la página Propiedades 184
  - creación en una vista de resultados 185
  - eliminación en la página Propiedades 185
  - modificación en la página Propiedades 185
- resultados por correo electrónico 222
- resultados solucionados/que faltan 175
  - personalizado 183
- rutina de validación
  - adición 239
    - específico de API 209
    - específico del sitio de llamada 209
- rutina de validación/codificación 240
- rutinas de codificación 198
- rutinas de validación 198
- rutinas específicas de API 198
- rutinas específicas de sitio de llamada 198

## S

- salida perdida 193, 195
- seguimiento de defectos 211
  - correo electrónico 222
  - HP Quality Center 216
    - envío de resultados a 216
    - información de resultados 217
    - seguimiento de resultados 216
  - IBM Rational ClearQuest 217
    - envío de defectos 218
  - Rational ClearQuest
    - envío de resultados 217
    - guardar defectos 221
  - Rational Team Concert 218
    - certificados SSL 104, 219
    - envío de defectos 219
  - Team Foundation Server 220
    - envío de defectos 220
- selección 145
  - con exclusiones 169
  - con paquetes 172
  - ejemplo 149
  - proceso 148
- seleccionar y ordenar columnas 216
- sink 193, 329
- Software Security Profile 225, 228
- Soporte a Common Weakness Enumeration 339
- Soporte a CWE 339
- soporte de anotaciones 188
- soporte de atributos 188
- sospechoso 242
- source 193, 329
- strncpy() 186, 329

## T

- Team Foundation Server 220
  - envío de defectos 220
- tipo de vulnerabilidad 151
- Tomcat 97
  - compilador 106

## V

- V/KLoC 313
- validación 192
  - específico de API 199
  - específico del sitio de llamada 199
- variables
  - definición 99, 141
    - cuando se publica y se guarda 142
    - ejemplo 142
- vi 187, 197
- vías de acceso absolutas 139
- visión general del producto 19
- vista Asesoramientos publicados 133, 135, 314
- Vista Asesoramientos publicados
  - suprimir 134
- Vista Asistencia de remediación 329
- vista Biblioteca de reglas de patrón 250, 295
- vista Configuración del escaneo 119, 255, 305
- vista Consola 312
- Vista de informe 323
- vista Detalle de resultado 178, 327
- vista Diferencia entre asesoramientos 148, 315
- Vista Editor de filtros 166, 332
- vista Explorador 84, 85, 259, 290, 299
- Vista Matriz de vulnerabilidad 332
- Vista Métricas 313
- vista Mis asesoramientos 313
  - gestión 127
- vista Paquetes 334
- Vista Paquetes 334
- Vista previa 231, 308
- vista Propiedades 84, 296
- Vista Rastreo 194, 329
- vista Reglas personalizadas 240, 247, 289
- vista Resultados 319
- Vista Resultados de la búsqueda 322
- Vista Resultados excluidos 321
- Vista Resultados modificados 321
- Vista Resultados personalizados 316
- Vista Resultados solucionados/ Ausentes 322
- Vista Resumen de asesoramiento 331
- vistas 289
  - asesoramiento 331
  - Asesoramientos publicados 314
  - Asistencia de remediación 329
  - Biblioteca de reglas de patrón 250, 295
    - con resultados 316
  - configuración 289
  - Configuración del escaneo 119, 255, 305
  - Consola 312



- vistas (*continuación*)
  - Detalle de resultado 178, 327
  - Diferencia entre asesoramientos 148, 315
  - Editor de filtros 332
  - Entradas y salidas 325
  - Explorador 84, 85, 259, 290, 299
  - investigación de resultados
    - únicos 326
  - Matriz de vulnerabilidad 332
  - Métricas 313
  - Mis asesoramientos 313
    - gestión 127
  - Paquetes 334
  - personalización 318
    - tabla de resultados 316
  - Propiedades 84, 296
  - Rastreo 194, 329
  - Reglas personalizadas 240, 247, 289
  - Report 323
  - Resultados 319
  - Resultados de la búsqueda 322
  - Resultados excluidos 321
  - Resultados modificados 321
  - Resultados personalizados 316
  - Resultados solucionados/ausentes 322
  - Resumen de asesoramiento 331
  - salida de escaneo 312
  - selección 315
- Visual Studio.NET 187, 197
- vulnerabilidad
  - definición 20
- vulnerabilidad de patrón de texto 247, 248

## W

- WebLogic 58, 98, 106, 259, 299
  - compilador 106
- WebSphere 98
- WebSphere Application Server 106
  - compilador 106







Impreso en España