

FIRMA DIGITAL

MANUAL DE
PROCEDIMIENTOS
PARA SOLICITANTES

ÍNDICE

Introducción a Firma Digital	Pag. 2
1) Requerimientos tecnológicos	Pag. 4
2) Instalación de AC-RAÍZ	Pag. 4
3) Instalación de AC-ONTI	Pag. 6
4) Solicitud por software	Pag. 8
a) Documentación a presentar	
b) Procedimiento de solicitud de certificado	
6) Solicitud por hardware	Pag. 13
a) Documentación a presentar	
b) Procedimiento de solicitud de certificado	
7) Revocación del certificado	Pag. 16

INTRODUCCIÓN

¿Qué es la firma digital?

La firma digital es una herramienta tecnológica que permite garantizar la autenticidad, integridad, exclusividad, no repudio y validez de los documentos digitales posibilitando que estos posean la misma característica que los documentos firmados mediante firma hológrafa (de puño y letra), exclusiva de los documentos en papel. Una firma digital es un conjunto de datos asociados a un mensaje digital que permite garantizar la identidad del firmante y la integridad del mensaje.

Cada titular de una firma digital posee un par de claves asociadas, una privada y otra pública, generada mediante un proceso matemático.

CLAVE PRIVADA: Es utilizada por su titular para firmar digitalmente un documento o mensaje, es secreta y mantenida por ese titular bajo su exclusiva responsabilidad.

CLAVE PÚBLICA: Es utilizada por el receptor de un documento o mensaje firmado para verificar la integridad y la autenticidad, asegurando el "no repudio".

Ambas claves se encuentran asociadas entre sí por las características especiales del proceso matemático.

Según la legislación argentina, si un documento firmado digitalmente es verificado correctamente, se presume, salvo prueba de lo contrario, que proviene del suscriptor del certificado asociado y que no fue modificado.

¿Qué son las Autoridades de Registro (AR)?

Las Autoridades de Registro (AR) son las responsables de efectuar las funciones de validación de identidad, de la titularidad de la clave pública asociada y de otros datos de los solicitantes y suscriptores de certificados digitales, de acuerdo al ámbito de aplicación establecido para cada una de ellas.

La provincia de Entre Ríos adhirió a la Ley Nacional de Firma Digital N° 25.506, mediante la Ley Provincial N° 10.425, reglamentada por Decreto N° 3825/16 MGyJ, a través del cual se dispone que el Ministerio de Gobierno y Justicia será la autoridad de aplicación y ejecución de la Ley N° 10.425.

EL Art. 8° del Decreto Reglamentario N° 3825/16 MGyJ dispone que las autoridades de registro (AR) sean el Ministerio de Gobierno y Justicia en la provincia de Entre Ríos, y la Secretaría de Modernización del Estado, Ciencia y Tecnología en el ámbito de la administración pública.

¿Quién es el Oficial de Registro (OR)?

El Oficial de Registro efectúa procedimientos con el fin de realizar la identificación del solicitante de firma digital y corroborar la titularidad de la solicitud de certificado:

- a) Verifica la existencia en el sistema de la solicitud, si correspondiese .
- b) Al momento de presentación del solicitante o suscriptor en sus oficinas, valida su identidad mediante la verificación de la documentación requerida.
- c) Verifica la titularidad de la solicitud mediante el control de la nota correspondiente, si fuera aplicable.
- d) De corresponder, requiere al solicitante la firma de la nota de solicitud en su presencia.
- e) Resguarda toda la documentación respaldatoria del proceso de validación de la identidad de los solicitantes y suscriptores de certificados, por el término de diez (10) años a partir de la fecha de vencimiento o revocación del certificado.

¿Qué son los certificados digitales?

Los certificados digitales son documentos digitales que dan fe de la vinculación entre una clave pública y un individuo o entidad. De este modo, permiten verificar que una clave pública específica pertenece, efectivamente, a un individuo determinado.

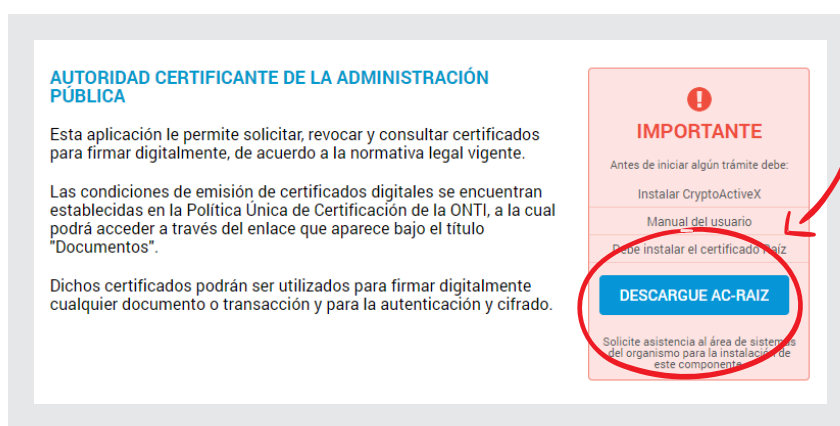
En su forma más simple el certificado contiene una clave pública y un nombre. Habitualmente, también contiene una fecha de expiración, el nombre de la Autoridad Certificante que la emitió, un número de serie y alguna otra información. Pero lo más importante es que el certificado propiamente dicho está firmado digitalmente por el emisor del mismo. En el caso de la provincia de Entre Ríos, el emisor es la Oficina Nacional de Tecnologías de la Información (ONTI).

Los Certificados con nivel de seguridad por software tienen la ventaja de no necesitar hardware especial y de no tener costos económicos posibilitando su uso masivo. Sólo requiere instalar el certificado en el ordenador que se utilizará para firmar digitalmente documentos. El sistema solicitará el ingreso de la clave privada para firmar documentos.

Por su parte, los Certificados con nivel de seguridad por hardware brindan una mayor seguridad ya que los datos privados del titular son almacenados en un dispositivo criptográfico especial (TOKEN). Para firmar digitalmente, el sistema solicitará que se conecte el dispositivo criptográfico y se ingrese la clave privada.

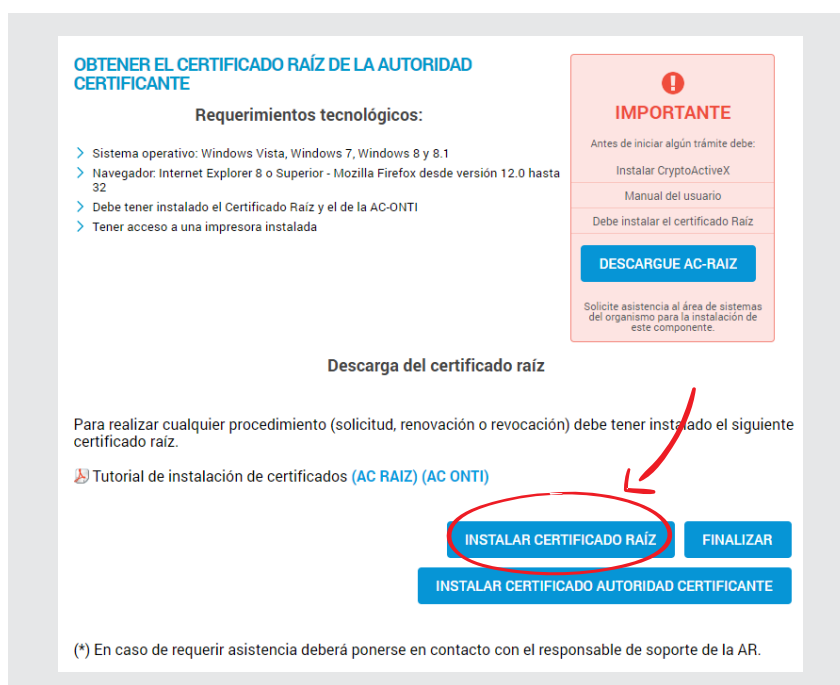
1 - REQUERIMIENTOS TECNOLÓGICOS PARA INICIAR EL TRÁMITE

- >> Sistema operativo Windows en sus versiones: Vista, 7, 8, 8.1 y 10.
- >> Navegador: Internet Explorer 8 o superior - Mozilla Firefox desde versión 12.0 en adelante
- >> Debe tener instalado el Certificado Raíz, que se podrá descargar de esta página:
<https://pki.jgm.gov.ar/app>

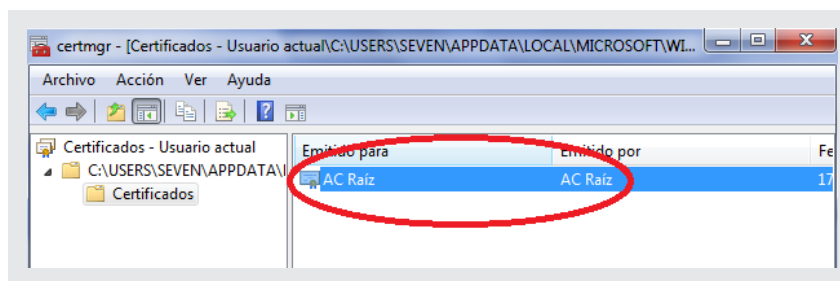


2 - INSTALACIÓN DEL CERTIFICADO AC-RAÍZ

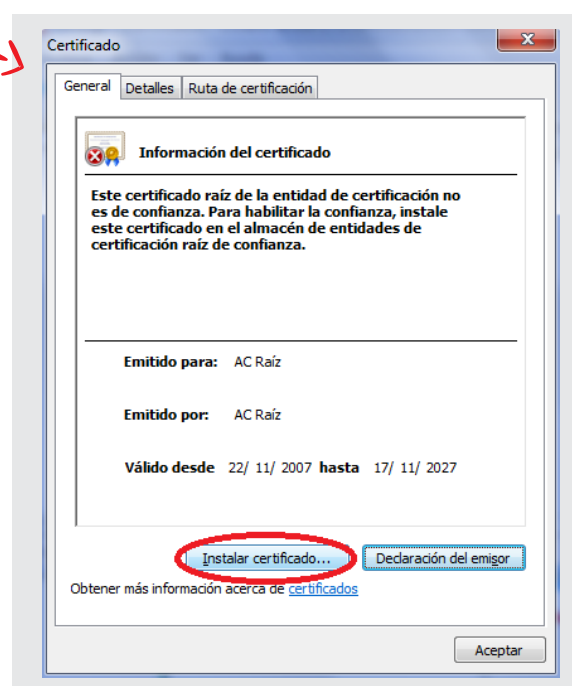
Una vez en la página ingresar en la pestaña "Certificados" y seleccionar la opción "Obtener el Certificado Raíz de la Autoridad Certificante". En la parte inferior hacer click en "Instalar Certificado Raíz" para descargarlo.



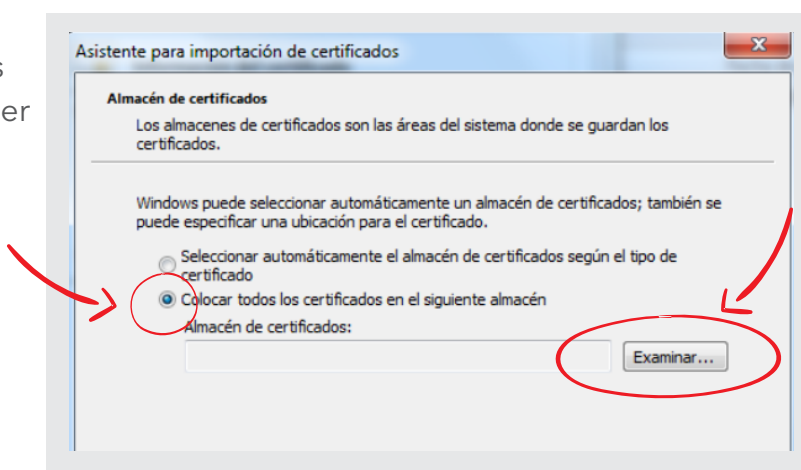
Una vez descargado, abrir el archivo y en la nueva ventana hacer click en "Certificados" y luego doble click en "AC Raíz".



Se desplegará la siguiente ventana. Seleccionar la opción "Instalar Certificado".

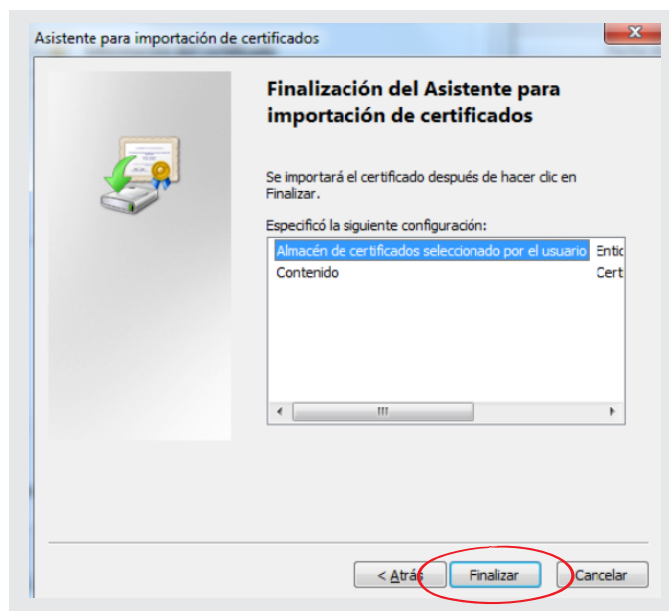
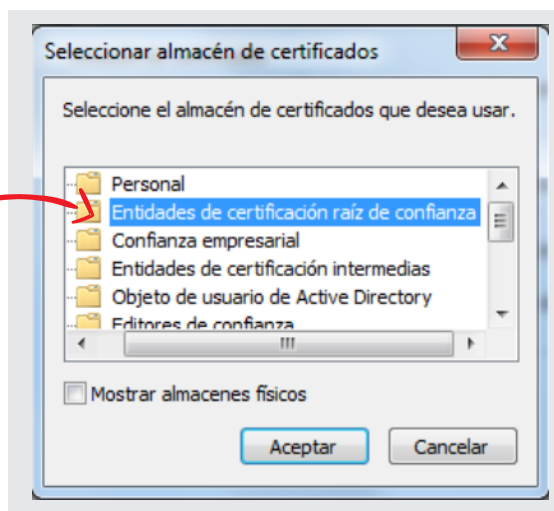


Seleccionar la opción "Colocar todos los certificados en el siguiente almacén" y hacer click en "Examinar".



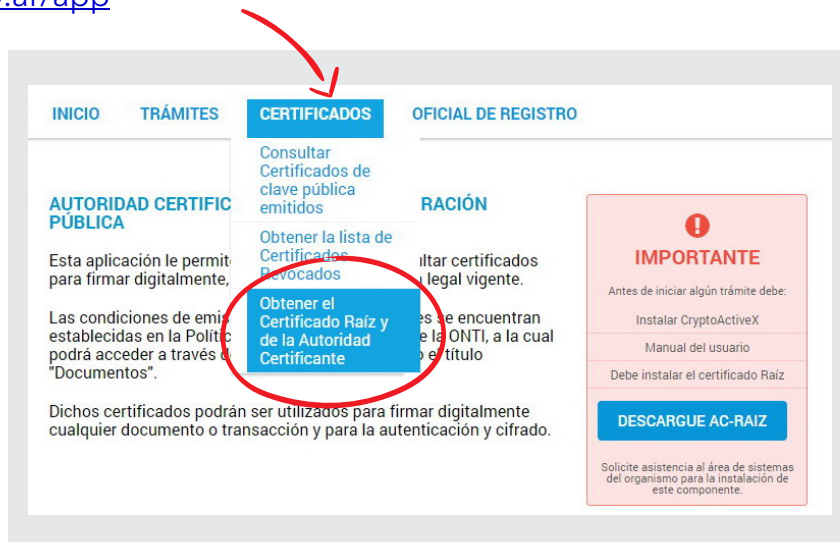
Seleccionar la carpeta "Entidades de certificación raíz de confianza" y hacer click en "Aceptar".

Hacer click en "Siguiente" y luego en "Finalizar".



3 - INSTALACIÓN DEL CERTIFICADO DE LA AC-ONTI

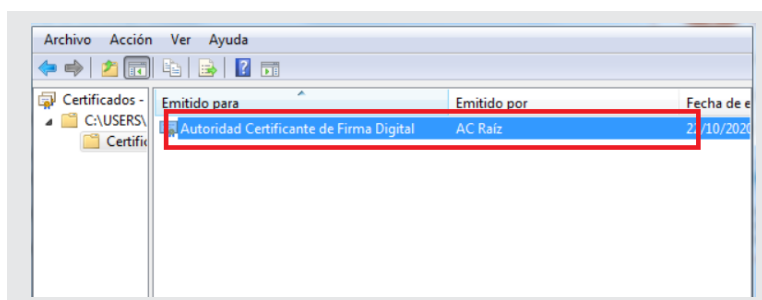
Debe tenerse instalado el certificado de la AC-ONTI, que podrá descargarse de la página: <https://pki.jgm.gov.ar/app>



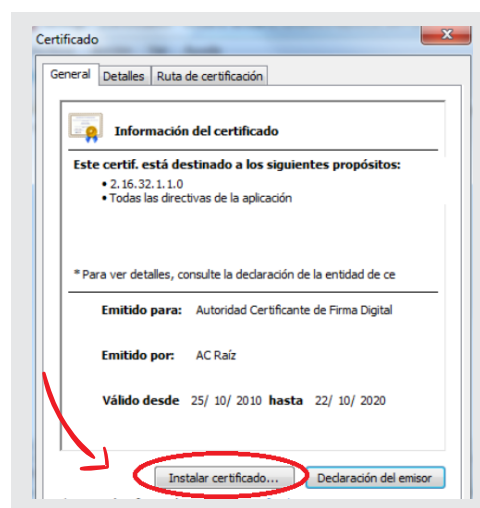
Hacer click en la parte inferior y seleccionar “Instalar Certificado Autoridad Certificante”.



Una vez descargado, abrir el archivo y en la nueva ventana hacer click en “Autoridad Certificante de Firma Digital”.

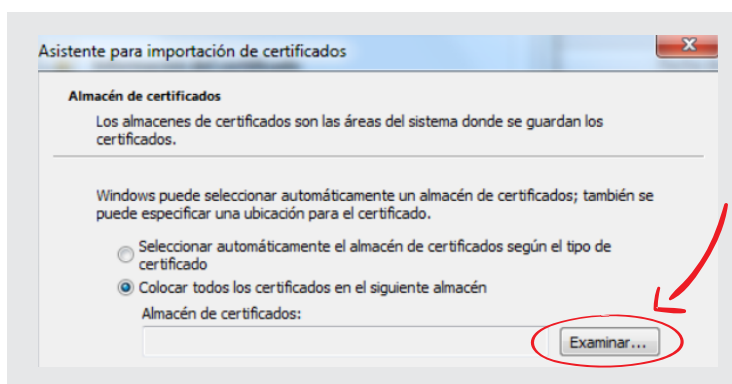
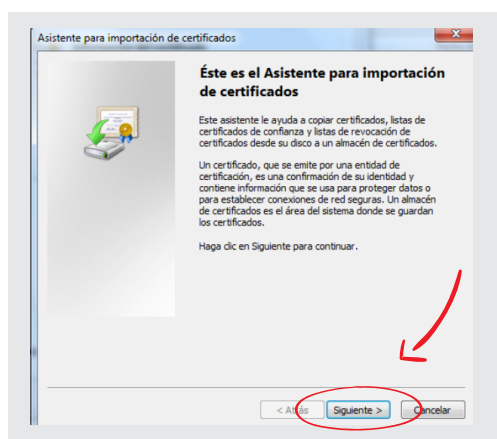


Luego hacer click en “Instalar certificado...”.

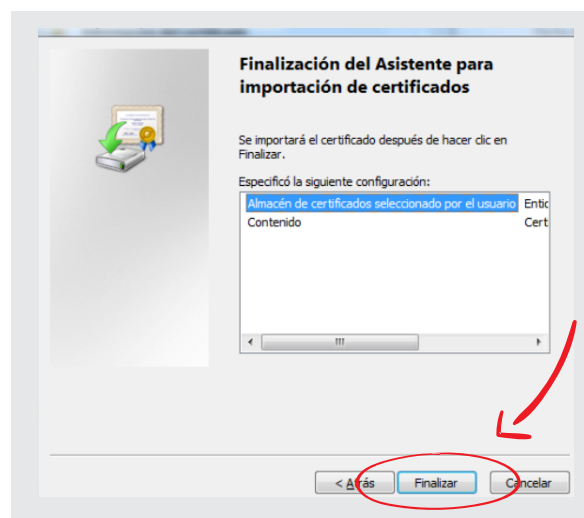
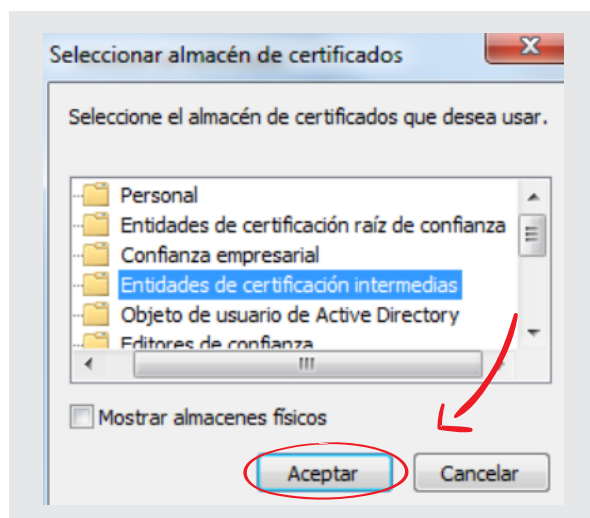


Una vez abierto el asistente presionar "Siguiente".

Seleccionar la opción "Colocar todos los certificados en el siguiente almacén" y luego en "Examinar".



Seleccionar la carpeta "Entidades de certificación intermedias" y hacer click en "Aceptar". Hacer click en "Siguiente" y después en "Finalizar".



4 - SOLICITUD POR SOFTWARE

a) Documentación

A continuación se detalla la documentación que el solicitante deberá reunir para solicitar su firma digital.

Persona Física:

>> DNI y fotocopia de DNI. En caso de extranjeros sin residencia en el país, presentar pasaporte válido u otro documento válido aceptado en virtud de acuerdos internacionales.

>> Constancia de CUIL.

>> De tratarse de persona física integrante de entes estatales deberá presentar una nota de certificación de servicios o copia autenticada del acto administrativo correspondiente a su designación, o una constancia emitida por la oficina de recursos humanos de su organismo, firmada por un funcionario responsable en la que conste lugar y fecha de emisión, nombre y apellido, DNI y cargo que ocupa en el organismo.

Descargar Nota de Certificación de servicios:

http://pki.jgm.gov.ar/docs/Nota_de_certificacion_de_servicios_RRHH.pdf.

>> En caso de tratarse de persona física no integrante de entes públicos estatales que requieran su certificado para efectuar trámites con el Estado a través de alguna AR autorizada por el Certificador, la AR deberá exigir toda la documentación indicada en los ítems anteriores a excepción del certificado de servicio. Será responsabilidad de cada AR determinar la documentación y los procedimientos de verificación adicionales que consideren necesarios para validar el resto de los datos del solicitante.

>> Nota de solicitud de certificado firmada. Por cuestiones de seguridad es fundamental que la nota sea firmada por el solicitante ni bien fue impresa y sus datos controlados. Si la nota está sin firmar al momento de presentar la documentación ante el Oficial de Registro (OR) la solicitud será automáticamente rechazada.

PROCEDIMIENTO DE LA SOLICITUD DEL CERTIFICADO

IMPORTANTE: La solicitud debe ser realizada en el ordenador y con el perfil de usuario que usará la firma digital. Mantener los recaudos necesarios.

1 - Realización de la solicitud

Para realizar la solicitud del certificado el usuario deberá ingresar al sitio web del certificador disponible en <https://pki.jgm.gov.ar/app>.

Una vez en la página acceder a la pestaña "Trámites", opción "Solicitud de Certificado".

INICIO **TRÁMITES** CERTIFICADOS OFICIAL DE REGISTRO

Solicitud de Certificado

AUTORIDAD PÚBLICA

Revocar Certificado con Clave Privada : LA ADMINISTRACIÓN

Revocar Certificado con Código de Revocación : revocar y consultar certificados lo a la normativa legal vigente.

Esta aplicación para firmar

Las conc Mis Trámites tificados digitales se encuentran establecidas en la Política Única de Certificación de la ONTI, a la cual podrá acceder a través del enlace que aparece bajo el título "Documentos".

Dichos certificados podrán ser utilizados para firmar digitalmente cualquier documento o transacción y para la autenticación y cifrado.

IMPORTANTE

Antes de iniciar algún trámite debe:

- Instalar CryptoActiveX
- Manual del usuario
- Debe instalar el certificado Raíz

DESCARGUE AC-RAIZ

Solicite asistencia al área de sistemas del organismo para la instalación de este componente.

Luego de leer lo detallado seleccionar al final de la página el tipo de persona: Física. En la página siguiente (al final) seleccionar la opción "Software".

En virtud de la Disposición de la SUBSECRETARÍA DE TECNOLOGÍAS DE GESTIÓN de la SECRETARÍA DE GABINETE de la JEFATURA DE GABINETE DE MINISTROS N° 11, de fecha 30 de diciembre de 2014, que aprueba la POLÍTICA ÚNICA DE CERTIFICACIÓN de la AUTORIDAD CERTIFICANTE de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN, en el apartado 1.3.3 se indica que podrán ser suscriptores de los certificados emitidos por la AC-ONTI:

- Las personas físicas que desempeñen funciones en entes públicos estatales.
- Las personas físicas o jurídicas que realicen trámites con el Estado, cuando existe una aplicación que requiera una firma digital, siempre que se cumplan las siguientes condiciones:
 - a) Deberá existir una AUTORIDAD DE REGISTRO autorizada por el Certificador en el organismo responsable de la aplicación, quien debe informar de la misma al Certificador.
 - b) Los solicitantes de certificados deberán efectuar el trámite de solicitud exclusivamente ante la AUTORIDAD DE REGISTRO autorizada.
- Los organismos y las empresas públicas.

TIPO DE PERSONA

FÍSICA

Cuando la solicitud es por SOFTWARE:

- El oficial de registro realiza las validaciones correspondientes y según sea el caso, aprueba o rechaza la solicitud. El sistema envía luego un correo electrónico a la dirección validada del solicitante informando la emisión del certificado y el link correspondiente para su descarga, o bien el eventual rechazo de la solicitud.

Cuando la solicitud es por HARDWARE:

- El oficial de registro realiza las validaciones correspondientes y el soporte técnico de firma digital verifica los requisitos del dispositivo criptográfico. Según sea el caso, el oficial de registro habilita a "solicitar certificado" para continuar con el trámite, o bien rechaza la solicitud.
- El solicitante valida los datos enviados (en el punto 1), inserta su dispositivo criptográfico y completa la solicitud, generando sus claves en el mismo. Imprime el formulario, verifica los datos impresos y lo firma.
- El oficial de registro aprobará la solicitud e instalará el certificado en el dispositivo, o eventualmente la rechazará. El sistema envía luego un correo electrónico a la dirección validada del titular, informando la emisión del certificado y poniendo a su disposición un enlace para futuras descargas.

RECUERDE: si durante la vigencia del plazo de validez de su certificado se produce alguna modificación en los datos incluidos en el mismo, usted deberá revocarlo y generar uno nuevo.

TIPO DE DISPOSITIVO CRIPTOGRÁFICO

SOFTWARE

HARDWARE (TOKEN)

Aparecerá una nueva página donde se encuentra el formulario de solicitud. Completar con los datos correspondientes (en caso de ser agente de la administración pública la información debe ser la misma que figura en la certificación de servicios). Una vez cumplido este paso leer detenidamente el acuerdo de suscriptores. Si el solicitante está de acuerdo tildar: **"Declaro haber leído y acepto el acuerdo con suscriptores"**. Luego ingresar el campo captcha con el código de seguridad y al final de la misma página clicar "Generar claves y solicitar certificado".

Se le preguntará al solicitante qué nivel de seguridad quiere para su firma (alto o medio). Hacer click en "Nivel de seguridad" y seleccionar **ALTO**.

Solicitud de certificado

Datos personales

(*) LOS CAMPOS SON OBLIGATORIOS

Nombres *
Como figura en el DNI

Apellidos *

Tipo de Documento *
Seleccione una opción

Número de documento *

País emisor *
Seleccione una opción

Cuit/Cuil *
12-12345678-1

DATOS DE LA ORGANIZACIÓN

Organización *
Si no aplica, ingresá N/A

Área de la que depende *
Si no aplica, ingresá N/A

Cargo/Función *
Si no aplica, ingresá N/A

Correo electrónico *

Provincia *
Seleccione una opción

Localidad *
Seleccione una opción

Aplicación
-- Ninguna --

Autoridad de Registro *
Seleccione una opción

ACUERDO CON SUSCRIPTORES

El presente acuerdo entre la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN (en adelante ONTI) y el suscriptor de un certificado digital emitido por la Autoridad Certificante de la ONTI (en adelante AC ONTI) determina los derechos y obligaciones de la partes respecto a la solicitud, aceptación y uso de los certificados emitidos en el marco de la Política Única de Certificación.

1. SOLICITUD DE CERTIFICADO Y DESCRIPCIÓN DE LOS CERTIFICADOS

Podrán ser suscriptores de los certificados emitidos por la AC ONTI los funcionarios, agentes públicos y las personas...

Código de seguridad

☐ Declaro haber leído y acepto el acuerdo con suscriptores.

Verifique que los datos ingresados sean correctos antes de continuar el trámite.

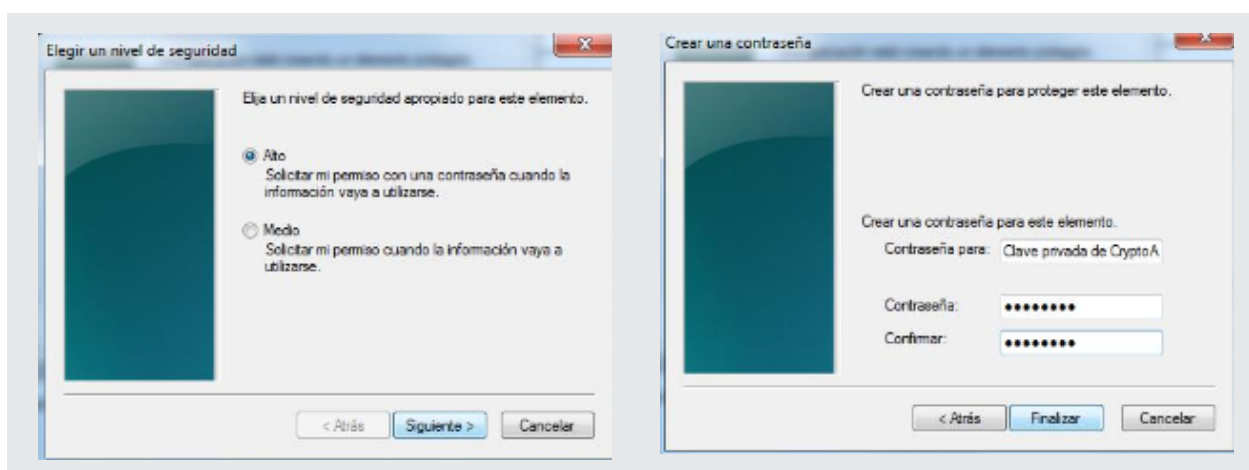
- La confirmación de los datos aquí consignados y la aceptación del Acuerdo con Suscriptores debe ser hecha por el propio titular de la solicitud y no por terceros de acuerdo con lo establecido en la Ley N° 25.506
- Una vez iniciado el trámite de solicitud debe ser concluido en la misma pc, con el mismo usuario y navegador.
- A partir de este momento hasta finalizar el trámite 'Verificación de datos', en caso de abandonar la estación de trabajo se deberá bloquear el equipo.

GENERAR CLAVES Y SOLICITAR CERTIFICADO **CANCELAR**

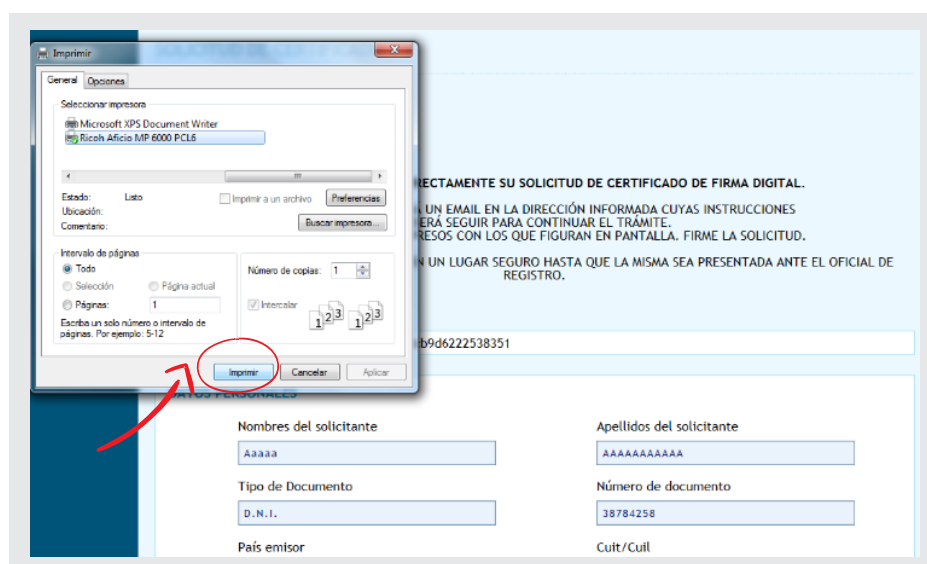
(*) Los campos son obligatorios

2 - Establecer contraseña

Se le pedirá al solicitante que establezca una contraseña. Crear una y hacer click en "Aceptar". Es importante recordar la contraseña y no compartirla con nadie, ya que con ella el solicitante procederá a firmar los documentos digitales.



Luego aparecerá una ventana que pregunta si se desea imprimir la solicitud. Imprimir la solicitud y firmar inmediatamente en el campo "Firma y aclaración del solicitante".



IMPORTANTE: La solicitud deberá ser firmada al momento de imprimirla ya que se ha generado la clave y en caso de no quedar resguardada, luego de ser impresa, puede ser modificada por terceros. En caso de no presentarse ante el OR con la nota de solicitud firmada, el certificado será rechazado y deberá realizar nuevamente el trámite.

3 - Verificación de la solicitud

La aplicación enviará un correo electrónico desde acap@sgp.gov.ar a la dirección que el solicitante indicó cuando completó el formulario de solicitud, conteniendo un link de verificación de la cuenta de correo. El solicitante deberá confirmar su correo para verificar la solicitud, haciendo click en "Confirmar recepción de mail".

4 - Contacto con el OR

El solicitante deberá contactarse con el Oficial de Registro (OR) de la Autoridad de Registro (AR) que le fue asignada, a fin de que le indique el procedimiento a seguir para presentar la documentación, incluyendo la nota de certificación de servicios y la nota de solicitud firmada por el solicitante.

5 - Emisión de certificado

Una vez cumplido el paso anterior y efectuada la aprobación de la solicitud por el OR, la Autoridad Certificante (AC) enviará un correo electrónico al solicitante informando la emisión del certificado y el link correspondiente para su descarga, junto al PIN de Revocación.

De acuerdo con lo establecido con la política de certificación y el manual de procedimientos, un suscriptor podrá revocar su certificado digital utilizando cualquiera de los siguientes métodos:

>> A través de la aplicación de la AC ONTI: <https://pki.jgm.gov.ar/app/> que se encuentra disponible veinticuatro (24) horas, si tiene acceso a su clave privada.

>> A través de la aplicación de la AC ONTI: <https://pki.jgm.gov.ar/app/> que se encuentra disponible veinticuatro (24) horas, utilizando el código de revocación que le fue entregado al momento de su solicitud.

5 - SOLICITUD POR HARDWARE

a) Documentación

Persona Física:

>> Presentar DNI y fotocopia de DNI. En caso de extranjeros sin residencia en el país, presentar pasaporte válido u otro documento aceptado en virtud de acuerdos internacionales.

>> Constancia de CUIL.

>> Constancia de CUIL.

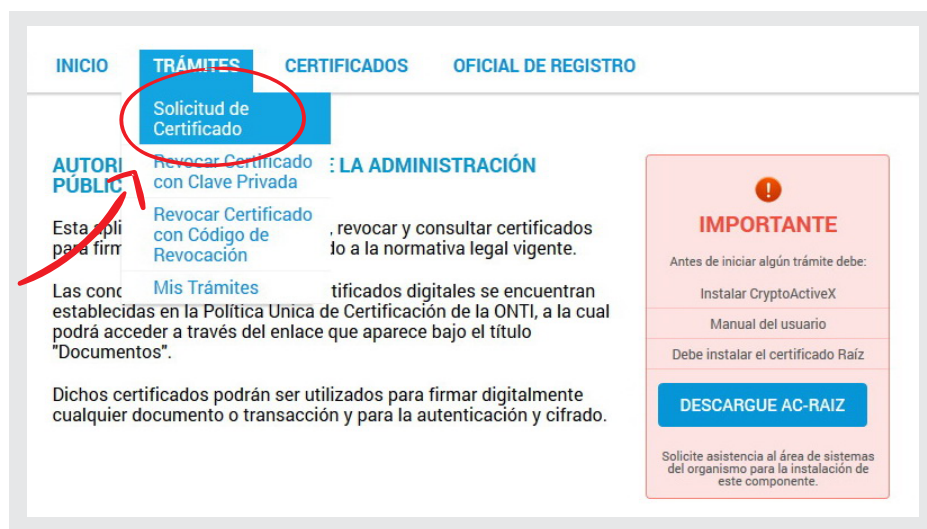
- De tratarse de persona física integrante de entes estatales deberá presentar una nota de certificación de servicios o copia autenticada del acto administrativo correspondiente a su designación, o constancia emitida por la oficina de recursos humanos y firmada por un funcionario responsable en la que conste lugar y fecha de emisión, nombre y apellido, DNI y cargo que ocupa en el organismo.
- En caso de tratarse de persona física no integrante de entes públicos estatales que requieran su certificado para efectuar trámites con el Estado a través de alguna AR autorizada por el Certificador, la AR deberá exigir toda la documentación indicada en los ítems anteriores a excepción del certificado de servicio. Será responsabilidad de cada AR determinar la documentación y los procedimientos de verificación adicionales que consideran necesarios para validar el resto de los datos de los solicitante
- Nota de envío de datos.
- Además, deberá presentarse con el dispositivo TOKEN.

PROCEDIMIENTO DE LA SOLICITUD DEL CERTIFICADO POR HARDWARE

IMPORTANTE: La solicitud debe ser realizada en el ordenador y con el usuario que usará la firma digital.

1 - Realización de la solicitud

Para realizar la solicitud del certificado el usuario debe ingresar al sitio web del Certificador disponible en <https://pki.jgm.gov.ar/app/>. Una vez en la página acceder a la pestaña "Trámites", opción "Solicitud de Certificado".



Luego de leer detenidamente lo detallado, seleccionar al final de la página el tipo de persona (Física) y la opción "Solicitud de Certificado".

En virtud de la Disposición de la SUBSECRETARÍA DE TECNOLOGÍAS DE GESTIÓN de la SECRETARÍA DE GABINETE de la JEFATURA DE GABINETE DE MINISTROS N° 11, de fecha 30 de diciembre de 2014, que aprueba la POLÍTICA ÚNICA DE CERTIFICACIÓN de la AUTORIDAD CERTIFICANTE de la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN, en el apartado 1.3.3 se indica que podrán ser suscriptores de los certificados emitidos por la AC-ONTI:

- ▶ Las personas físicas que desempeñen funciones en entes públicos estatales.
- ▶ Las personas físicas o jurídicas que realicen trámites con el Estado, cuando existe una aplicación que requiera una firma digital, siempre que se cumplan las siguientes condiciones:
 - a) Deberá existir una AUTORIDAD DE REGISTRO autorizada por el Certificador en el organismo responsable de la aplicación, quien debe informar de la misma al Certificador.
 - b) Los solicitantes de certificados deberán efectuar el trámite de solicitud exclusivamente ante la AUTORIDAD DE REGISTRO autorizada.
- ▶ Los organismos y las empresas públicas.

TIPO DE PERSONA

FÍSICA

Seleccionar en la página siguiente la opción "Hardware".

Cuando la solicitud es por HARDWARE:

- 2 El oficial de registro realiza las validaciones correspondientes y el soporte técnico de firma digital verifica los requisitos del dispositivo criptográfico. Según sea el caso, el oficial de registro habilita a "solicitar certificado" para continuar con el trámite, o bien rechaza la solicitud.
- 3 El solicitante valida los datos enviados (en el punto 1), inserta su dispositivo criptográfico y completa la solicitud, generando sus claves en el mismo. Imprime el formulario, verifica los datos impresos y lo firma.
- 4 El oficial de registro aprobará la solicitud e instalará el certificado en el dispositivo, o eventualmente la rechazará. El sistema envía luego un correo electrónico a la dirección validada del titular, informando la emisión del certificado y poniendo a su disposición un enlace para futuras descargas.

RECUERDE: si durante la vigencia del plazo de validez de su certificado se produce alguna modificación en los datos incluidos en el mismo, usted deberá revocarlo y generar uno nuevo.

TIPO DE DISPOSITIVO
CRIPTOGRÁFICO

SOFTWARE

HARDWARE (TOKEN)

Aparecerá una nueva página donde se encuentra el formulario de solicitud que deberá ser completado por el solicitante con los datos correspondientes. Una vez cumplido este paso leer el acuerdo de suscriptores. Si el solicitante está de acuerdo tildar: "Declaro haber leído y acepto el acuerdo con suscriptores" y completar el captcha de seguridad con el código que aparece en pantalla. Verificar que los datos ingresados sean correctos antes de continuar el trámite y luego clicar la opción "Enviar datos de solicitud del certificado".



Ministerio de Modernización
Presidencia de la Nación

INICIO TRÁMITES CERTIFICADOS OFICIAL DE REGISTRO

Nota de envío de datos

Datos personales

(*) LOS CAMPOS SON OBLIGATORIOS

Nombres *	Apellidos *
Como figura en el DNI	
Tipo de Documento *	Número de documento *
Seleccione una opción	
País emisor *	Cuit/Cuil *
Seleccione una opción	12-12345678-1

DATOS DE LA ORGANIZACIÓN

Organización *	Área de la que depende *
Si no aplica, ingrese N/A	Si no aplica, ingrese N/A
Cargo/Función *	Correo electrónico *
Si no aplica, ingrese N/A	
Provincia *	Localidad *
Seleccione una opción	Seleccione una opción
Aplicación	Autoridad de Registro *
-- Ninguna --	Seleccione una opción

ACUERDO CON SUSCRIPTORES

El presente acuerdo entre la OFICINA NACIONAL DE TECNOLOGÍAS DE INFORMACIÓN (en adelante ONTI) y el suscriptor de un certificado digital emitido por la Autoridad Certificante de la ONTI (en adelante AC ONTI) determina los derechos y obligaciones de la partes respecto a la solicitud, aceptación y uso de los certificados emitidos en el marco de la Política Única de Certificación.

1. SOLICITUD DE CERTIFICADO Y DESCRIPCIÓN DE LOS CERTIFICADOS

Podrán ser suscriptores de los certificados emitidos por la AC ONTI los funcionarios, agentes públicos y las personas...

 Código de seguridad

☐ Declaro haber leído y acepto el acuerdo con suscriptores.

⚠ Verifique que los datos ingresados sean correctos antes de continuar el trámite.

ENVIAR DATOS DE SOLICITUD DE CERTIFICADO CANCELAR

(*) Los campos son obligatorios

2 - Imprimir la nota de envío de datos

Aparecerá una ventana en la que se le pregunta al solicitante si desea imprimir la nota de envío de datos. Imprimir la nota y firmar en el campo "Firma y aclaración del solicitante".

3 - Verificación de la solicitud

La aplicación enviará un correo electrónico desde acap@sgp.gov.ar a la dirección de correo que el solicitante indicó cuando completó el formulario de solicitud, conteniendo un link de verificación de la cuenta de correo. El solicitante deberá confirmar su cuenta de correo electrónico para verificar la solicitud, haciendo click en "Confirmar recepción de mail".

4 - Contacto con el OR

El solicitante deberá ponerse en contacto con un Oficial de Registro (OR) de la Autoridad de Registro en la cual comenzó el trámite y presentarse con la documentación anteriormente detallada, más una nota de certificación de servicios, una nota de envío de datos y el token.

5 - Emisión de certificado

Una vez cumplido el paso anterior y efectuada la aprobación de la solicitud por el OR, la Autoridad Certificante (AC) enviará un correo electrónico al solicitante informando la emisión del certificado y el link correspondiente para su descarga, junto al PIN de Revocación.

IMPORTANTE: En el momento de la descarga del certificado el Dispositivo Criptográfico (Token) deberá estar colocado en el ordenador. En caso de no haber seguido este procedimiento, el certificado automáticamente se guardará en la CPU del ordenador. Dado que los certificados no son exportables, no podrá ser incorporado al dispositivo criptográfico. En ese caso se deberá revocar el certificado y solicitarlo nuevamente.

6- REVOCACIÓN DE CERTIFICADOS

Causas de Revocación

>> A solicitud del titular del certificado digital o del responsable autorizado para el caso de certificados de personas jurídicas o aplicación.

>> Si se determina que el certificado fue emitido en base a información falsa, que al momento de la emisión hubiera sido objeto de verificación.

- >> Si se determina que los procedimientos de emisión y/o verificación han dejado de ser seguros.
- >> Por resolución judicial.
- >> Por resolución de la autoridad de aplicación.
- >> Por fallecimiento del titular.
- >> Por declaración judicial de ausencia con presunción de fallecimiento del titular.
- >> Por declaración judicial de incapacidad del titular.
- >> Si se determina que la información contenida en el certificado ha dejado de ser válida.
- >> Cuando la clave privada asociada al certificado, o el medio en que se encuentre almacenada se encuentren comprometidos o corran peligro de estarlo.
- >> Ante incumplimiento por parte del suscriptor de las obligaciones establecidas en el acuerdo de suscriptores.
- >> Si se determina que el certificado no fue emitido de acuerdo a los lineamientos de la Política Única de Certificación, del presente Manual de Procedimientos, de la Ley N° 25.506, el Decreto Reglamentario N° 2628/02 y demás normativa sobre firma digital.
- >> Por revocación de su propio certificado digital.

El certificado, de corresponder, revocará el certificado en un plazo no superior a las veinticuatro (24) horas de recibido el requerimiento de revocación.

Autorizados a solicitar la revocación

- >> El suscriptor del certificado.
- >> El responsable autorizado que efectuara el requerimiento, en el caso de certificados de personas jurídicas o aplicación.
- >> El responsable autorizado por la persona jurídica responsable del sitio web, en el caso de certificados de sitio seguro.
- >> Aquellas personas habilitadas por el suscriptor del certificado a tal fin, previa acreditación fehaciente de tal autorización.
- >> El certificador o la AR operativamente vinculada.
- >> El ente licenciante.
- >> La autoridad judicial competente.
- >> La autoridad de aplicación.

Procedimiento para la solicitud de revocación

- a) Se identifica debidamente al solicitante de la revocación.
- b) Las solicitudes de revocación, así como toda acción efectuada por el Certificador o la autoridad de registro en el proceso, están documentadas y conservadas en sus archivos.

- c) Se documentan y archivan las justificaciones de la revocaciones aprobadas.
- d) Una vez efectuada la revocación, se actualiza el estado del certificado en el repositorio y se incluye en la próxima lista de certificados revocados a ser emitida.
- e) El suscriptor del certificado revocado es informado del cambio de estado de su certificado.

Un suscriptor podrá revocar su certificado digital utilizando cualquiera de los siguientes métodos:

- >> A través de la aplicación de la AC ONTI: <https://pki.jgm.gob.ar/app/>, que se encuentra disponible las 24 horas si tiene acceso a su clave privada.
- >> A través de la aplicación de la AC ONTI: <https://pki.jgm.gob.ar/app/>, utilizando el código de revocación que le fue entregado al momento de la emisión del certificado.
- >> En caso de no poder utilizar algunas de las opciones anteriores deberá presentarse ante la AR correspondiente con el DNI que permita acreditar su identidad.
- >> En caso de suscriptores pertenecientes a entes públicos estatales la revocación podrá ser solicitada por un responsable autorizado del organismo en el que se desempeña el titular del certificado, por nota dirigida al responsable de la AR.

Los suscriptores serán notificados en sus respectivas direcciones de correo electrónico o en la aplicación del Certificador del cumplimiento del proceso de revocación.

IMPORTANTE: Ante cualquier duda comunicarse con el responsable de Soporte Técnico de su Autoridad de Registro.

Elaborado por la Secretaría de Modernización del Estado, Ciencia y Tecnología

Secretaría General de la Gobernación
Gobierno de Entre Ríos
Enero de 2018