AGENCIA PARA LA REINCORPORACIÓN Y LA NORMALIZACIÓN (ARN)

MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI

BOGOTÁ D.C. JUNIO DE 2018

TABLA DE CONTENIDO

INTRODUCCIÓN

La Agencia para la Reincorporación y la Normalización considera que la información es uno de sus principales activos intangibles indispensable en el cumplimiento de su misión y en la dirección y consecución de sus objetivos, programas, planes, proyectos y metas, por lo que se hace necesario establecer estrategias y mecanismos que nos permitan protegerla independientemente del medio en que se encuentre o la forma en que se maneje, transporte o almacene.

En este documento se describen las políticas, lineamientos y normas de seguridad de la información definidas por la ARN y se convierten en la base para la implantación de los estándares, procedimientos, instructivos y controles que deberán ser implementados por toda la entidad.

La seguridad de la información es una prioridad para la ARN y por tanto es responsabilidad de todos velar por el cumplimiento de cada una de estas políticas y lineamientos.

I. DE LA SEGURIDAD DE LA INFORMACIÓN

1.1. OBJETIVO

Establecer las directrices, lineamientos de seguridad y protección de la información, a través de la gestión segura de los activos de información, del Sistema de Gestión de Seguridad de la información, que contribuya al cumplimiento de las metas estratégicas de la Agencia.

1.2. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN -SGSI

El Sistema de Gestión de Seguridad de la Información-SGSI debe ser aplicado en todos los activos de información de la Agencia para la Reincorporación y la Normalización - ARN, en sus plataformas tecnológicas y en sus procesos.

(a) Activos de información
Dentro del alcance del SGSI están:

- los activos de información identificados y clasificados en los procesos de la ARN,
- sus directivos, colaboradores y contratistas.

(b) Plataformas tecnológicas

Las plataformas tecnológicas relevantes que hacen parte del alcance del SGSI se refiere a los sistemas de información, aplicativos, portales y/o servicios de Tecnologías de la Información de la Entidad.

(c) Procesos

Hacen parte del alcance del SGSI todos los procesos descritos en el mapa de procesos de la Agencia para la Reincorporación y la Normalización, que están clasificados en procesos estratégicos, procesos de evaluación, procesos misionales y procesos de apoyo.

El SGSI estará incorporado dentro del Sistema Integrado de Gestión para la Reintegración – SIGER y es responsable su adopción el Comité Institucional de Gestión y desempeño o quien haga sus veces.

1.3. DEFINICIONES

Activo: Según [ISO/IEC 13335-12004]: Cualquier cosa que tiene valor para la organización. También se entiende por cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.

Es todo activo que contiene información, la cual posee un valor y es necesaria para realizar los procesos misionales y operativos de la ARN. Se pueden clasificar de la siguiente manera:

- **Datos**: Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la ARN, así como cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Ejemplo: archivo de Word “Control Asistencia.docx”.
- **Hardware**: Son todos los equipos utilizados para gestionar la información y las comunicaciones. Ejemplo: servidores, switches, equipo de cómputo, impresoras, escáner.
- **Software**: son todas las herramientas, aplicativos, sistemas de información o portales que se utilizan para le gestión de la ARN. Se subdividen en:
  - **Aplicaciones:** Es todo el software que se utiliza para la gestión de la información. Ejemplo: Procesador de texto, herramienta para apoyo a la gestión, software para intercambio de información con otra entidad. Por ejemplo: SIGOB, SIGER.

- **Herramientas:** son programas o aplicaciones que pueden ser utilizadas por muchas personas para poyo a la gestión. Por ejemplo: procesador de palabra, gestor de proyectos, procesador de cálculo. Por ejemplo: Word, Excel, Atlas TI.
- **Sistemas de Información**: Son fuente única de datos útiles para apoyar o argumentar las decisiones corporativas. Incluyen estrategia, procesos, organización, recursos (humanos, tecnológicos, financieros), información confiable, entre otros. Por ejemplo: Sistema de Información para la reintegración – SIR.
- **Portales:** En Internet, conjunto de páginas reunidas bajo una marca, dirección, tema, asunto o interés. Por ejemplo: Portal Web de la ARN. – Colaboradores: Son todos los funcionarios, contratistas, pasantes y terceros que tengan acceso de una manera u otra a los activos de información de la ARN. Ejemplo: Asistente de Información Grupo territorial, contratista Grupo Contratación, Proveedor servicio de seguridad.
- **Servicios:** Son los servicios internos se refiere a los que se suministran internamente entre las dependencias de una organización y los externos, aquellos que la organización suministra a clientes y usuarios externos. Ejemplo: Publicación la ARN en Cifras.

ACTIVO DE INFORMACIÓN: Es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la entidad.

ADMINISTRACIÓN DE RIESGOS: Conjunto de Elementos de Control que, al interrelacionarse, permiten a la entidad pública evaluar aquellos eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales o los eventos positivos, que permitan identificar oportunidades para un mejor cumplimiento de su función. Se constituye en el componente de control que al interactuar sus diferentes elementos le permite a la entidad pública autocontrolar aquellos eventos que pueden afectar el cumplimiento de sus objetivos.

AMENAZA: Según [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

ANÁLISIS DE RIESGOS: Según [ISO/IEC Guía 73:2002]: Uso sistemático de la información para identificar fuentes y estimar el riesgo.

ANONIMIZACIÓN: Hace referencia al proceso por el cual deja de ser posible establecer, por medios razonables, el nexo entre un dato y el sujeto al que se refiere.
ANONIMIZAR: Hacer que una persona, obra o acción sean anónimos.

APLICACIONES: Es todo el software que se utiliza para la gestión de la información.

ATAQUE CIBERNÉTICO: Acción organizada o premeditada de una o más agentes para causar daño o problemas a un sistema a través del Ciberespacio.

AUTENTICACIÓN: Proceso que tiene por objeto asegurar la identificación de una persona o sistema.

AUTENTICIDAD: Los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso.

AUTORIZACIÓN: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

BASE DE DATOS: Conjunto organizado de datos personales que sea objeto de Tratamiento.

BASE DE DATOS AUTOMATIZADA: Es aquella que se almacena y administra con la ayuda de herramientas informáticas.

BASE DE DATOS MANUAL O ARCHIVO: Son aquellas cuya información se encuentra organizada y almacenada de manera física, como las hojas de vida de los funcionarios.

BIG DATA: Conjunto de herramientas informáticas destinadas a la manipulación, gestión y análisis de grandes volúmenes de datos de todo tipo.

CIBERCRÍMEN (DELITO CIBERNÉTICO): Conjunto de actividades ilegales asociadas con el uso de las Tecnologías de la Información y las Comunicaciones, como fin o como medio.

CIBERLAVADO: Uso del Ciberespacio, en cualquiera de sus formas, para dar apariencia de legalidad a bienes obtenidos ilícitamente o para ocultar dicha ilicitud ante las autoridades.

CIBERSEGURIDAD: Conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio.

CIBERDEFENSA: Empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales.

CIBERESPIONAJE: Acto o práctica de obtener secretos sin el permiso del dueño de la información (personal, sensible, propietaria o de naturaleza clasificada) para ventaja personal, económica, política o militar en el Ciberespacio, a través del uso de técnicas malintencionadas.

CIBERTERRORISMO: Uso del Ciberespacio como fin o como medio, con el propósito de generar terror o miedo generalizado en la población, nación o estado trayendo como consecuencia una violación a la voluntad de las personas.

COLCERT: Grupo de Respuesta a Emergencias Cibernéticas de Colombia

COMPROMISO DE LA DIRECCIÓN: Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI.

CONFIABILIDAD: Propiedad de tener comportamientos y resultados previstos consistentes.

CONFIDENCIALIDAD: Acceso a la información por parte únicamente de quien esté autorizado. Según [ISO/IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

CONTROL: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. (Nota: Control es también utilizado como sinónimo de salvaguarda).

CSIRT: Equipos de Respuestas ante Incidentes de Seguridad (en inglés, Computer Security Incident Response Team)

DATO: Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la ARN.

DATO PERSONAL: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables;

DATO PÚBLICO: Según tipología por protección de datos personales, es el dato que la ley o la Constitución Política determina como tal, así como todos aquellos que no sean semiprivados o privados.

DATO SEMIPRIVADO: Según tipología por protección de datos personales, es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas.

DATO PRIVADO: Según tipología por protección de datos personales, es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular de la información.

DATO SENSIBLE: según tipología por protección de datos personales, es el dato que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

DERECHO DE HABEAS DATA: El derecho de hábeas data es aquel que tiene toda persona de conocer, actualizar y rectificar la información que se haya recogido sobre ella en archivos y bancos de datos de naturaleza pública o privada.

DESASTRE: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

DISPONIBILIDAD: Los activos de información deben estar disponibles para soportar la misión de la ARN.

ENCARGADO DEL TRATAMIENTO: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento;

EVENTO: Según [ISO/IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardias, o una situación anterior desconocida que podría ser relevante para la seguridad.

GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL: Conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego.

GUSANO: Es un programa de computador que tiene la capacidad de duplicarse a sí mismo. A diferencia del virus, no precisa alterar los archivos de programas, sino que reside en la memoria y se duplica a sí mismo. Siempre dañan la red (aunque sea simplemente consumiendo ancho de banda).

IMPACTO: Resultado de un incidente de seguridad de la información.

INCIDENTE: Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

INFORMACIÓN: Constituye un importante activo, esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada. Puede existir de muchas maneras. Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, exponer oralmente, audiovisual u otro.

INGENIERÍA SOCIAL: Es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales, o delincuentes informáticos, para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos.

INSTALACIONES: Son todos los lugares en los que se alojan los sistemas de información.

INTEGRIDAD: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISO/IEC 13335-1:2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos. Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

INTELIGENCIA DE NEGOCIOS (Business Intelligence-BI): Es el conjunto de técnicas, procesos y arquitectura que transforman los datos recopilados por una organización, entidad o compañía en información importante y relevante para los procesos gerenciales, desde la disminución de costos, hasta la creación de nuevos negocios, establecimiento de políticas, planes o lineamientos.

INVENTARIO DE ACTIVOS: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación, de la entidad, etc.), dentro del alcance del Sistema de Gestión de Seguridad de la Información – SGSI que tengan valor para la entidad y necesiten por tanto ser protegidos de potenciales riesgos.

KEYLOGGERS: software o aplicaciones que almacenan información digitada mediante el teclado de un computador por un usuario, que actúa como un proceso información que no interactúa con el usuario ya que se ejecuta en segundo plano.

MESA DE SEGURIDAD: La Mesa de Seguridad tiene como objeto Coordinar y Asesorar al Comité Institucional de Gestión y desempeño o quien haga sus veces, en los temas de seguridad física y de infraestructura, seguridad de la información y Seguridad de la población objeto de atención por parte de la ARN. La coordinación y asesoría realizada por la Mesa de Seguridad no suplanta las responsabilidades asignadas al Asesor de Seguridad de la Secretaría General, al profesional de seguridad informática de la Oficina de Tecnologías de la Información y el

funcionario o contratista responsable de los temas de Seguridad Misional de la Dirección Programática de la Agencia para la Reincorporación y la Normalización.

NO REPUDIO: Se debe tener la capacidad para probar que una acción o un evento relacionados con los activos de información han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.

OPEN DATA: Es la apertura de datos públicos y consiste en poner la información que posee el sector público al alcance de todo el mundo en formatos digitales, estandarizados y abiertos, siguiendo una estructura clara que permita su comprensión y para su reutilización.

PHISHING: Tipo de delito encuadrado dentro del ámbito de las estafas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).

POLÍTICA DE SEGURIDAD: Documento que establece el compromiso de la Dirección y el enfoque de la entidad en la gestión de la seguridad y privacidad de la información.

PROTECCIÓN DE DATOS PERSONALES: Son todas las medidas que se toman, tanto a nivel procedimental, técnico como jurídico, para garantizar que la información de los usuarios de una entidad o de cualquier base de datos, esté segura de cualquier ataque o intento de acceder a esta, por parte de personas no autorizadas.

RANSONWARE: Es un software malicioso que al infectar el equipo le da al ciber delincuente la capacidad de bloquearlo desde una ubicación ajena al usuario y encriptar la información no permitiendo el acceso a la misma.

RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN: Es el Comité Institucional de Gestión y Desempeño o quien haga sus veces que cumple la función de supervisar el cumplimiento de los temas relacionados con seguridad de la información del SGSI.

RESPONSABLE DE SEGURIDAD INFORMÁTICA: Es la persona que cumple la función de supervisar el cumplimiento de los temas relacionados con seguridad informática y de asesorar en dicho tema a los integrantes de la Entidad que así lo requieran.

RESPONSABLE DEL TRATAMIENTO: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos;

RIESGO: Posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.

RIESGO CIBERNÉTICO: Es el efecto de incertidumbres sobre objetivos y puede resultar de eventos en donde las amenazas cibernéticas se combinan con vulnerabilidades generando consecuencias económicas.

RIESGO DE SEGURIDAD DIGITAL: Es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. El riesgo de seguridad digital es de naturaleza dinámica. Incluye aspectos relacionados con el ambiente físico y digital, las personas involucradas en las actividades y los procesos organizacionales que las soportan.

RNBD: Registro Nacional de Bases de Datos de la Superintendencia de Industria y Comercio para la protección de datos personales.

SEGURIDAD DE LA INFORMACIÓN: Según [ISO/IEC 27002:2013]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.

SGSI SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN: Según [ISO/IEC 27001: 2013]: la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. Incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos. En cuanto a protección incluye dentro del sistema la normativa de protección de datos personales.

SPAMMING: Se llama spam, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades

(incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. La vía más usada es el correo electrónico.

SNIFFERS: Programa de captura de las tramas de red. Generalmente se usa para gestionar la red con una finalidad docente o de control, aunque también puede ser utilizado con fines maliciosos.

SPOOFING: Falsificación de la identidad origen en una sesión: la identidad es por una dirección IP o dirección MAC.

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO – SIC: Autoridad nacional de la propiedad industrial y defiende los derechos fundamentales relacionados con la correcta administración de datos personales.
TITULAR: Persona natural cuyos datos personales sean objeto de Tratamiento;

TRATAMIENTO: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

TROYANO: Aplicación que aparenta tener un uso legítimo pero que tiene funciones ocultas diseñadas para sobrepasar los sistemas de seguridad.

USUARIO: en el presente documento se emplea para referirse a los colaboradores (directivos, funcionarios, contratistas, pasantes y terceros) de la ARN, debidamente autorizados para usar equipos, sistemas o aplicativos o servicios informáticos, disponibles en la red de la ARN y a quienes se les otorga un nombre de usuario y una clave de acceso.

VIRUS: tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o conocimiento del usuario.

VULNERABILIDAD: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 133351:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza

II. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La Dirección General de la ARN aprueba esta política de Seguridad de la Información como muestra de su compromiso en la protección de su información.

2.1. COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO O QUIEN HAGA SUS VECES

Para la adecuada dirección, implementación, implantación, gestión y mantenimiento del SGSI y de la Política de Gobierno Digital en la ARN se requiere la intervención del Comité. En el marco del cual se creó una Mesa de trabajo de Seguridad como una instancia de discusión, asesoría y coordinación de los diferentes temas relativos a la seguridad de la infraestructura física, de los funcionarios, de la información y la misional de la ARN. Es el ente interdisciplinario, constituido con el fin de lograr acciones efectivas en el marco del SGSI y de la Política de Gobierno Digital, contando con el apoyo de la Alta Dirección.

La Mesa de Seguridad estará conformada por:

- El Asesor de Seguridad del Despacho de la Dirección General, como delegado del director, quien lo liderará asumiendo así el rol de Oficial de Seguridad de la Información
- El Asesor de Seguridad de la Secretaría General como delegado del Secretario General
- El Profesional de Seguridad Informática de la Oficina de Tecnologías de la Información,
- Un delegado de la Dirección Programática (Encargado de los temas de seguridad misionales en la DPR)
- Un delegado de la Oficina Asesora de Planeación
- Un delegado de la Oficina Asesora Jurídica
- Un delegado de Talento Humano para el tema de Seguridad y Salud en el Trabajo
- Un delegado de Gestión documental

2.2. ASIGNACIÓN DE RESPONSABILIDADES

El Comité Institucional de Gestión y Desempeño o quien haga sus veces es el responsable de:

- Orientar las políticas del SGSI
- Coordinar los procedimientos de seguridad

- Liderar y orientar la implementación de la Política de Gobierno Digital de acuerdo con el Decreto 1008 de 2018 y conforme a lo establecido en el Modelo Integrado de Planeación y Gestión - MIPG.
- Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información.
- Hacer seguimiento a los planes de seguridad

La Mesa de Seguridad está encargada de la articulación, coordinación, análisis y estudio de las siguientes temáticas:

- Seguridad de servidores públicos, contratistas e infraestructura de la ARN
- Sistema de Gestión de Seguridad de la Información

Las funciones de la Mesa de Seguridad son:

- Articular las acciones que en materia de seguridad desarrolle la Agencia para la Reincorporación y la Normalización.
- Emitir recomendaciones en cuanto el establecimiento de medidas o políticas relativas al tema de seguridad.
- Realizar seguimiento a las novedades de seguridad física, de funcionarios y contratistas, así como de las personas objeto de atención.
- Evaluar y retroalimentar los planes de seguridad desarrollados por cada una de las dependencias responsables.
- Establecer un acuerdo de trabajo anual en materia de seguridad.
- Reportar a través de su coordinador los temas que deban ser tratados y aprobados en plenaria del Comité Institucional de Gestión y Desempeño o quien haga sus veces, lo anterior, con el fin de establecer la agenda de las sesiones del Comité.

Coordinador de la Mesa de Seguridad:

El responsable de la Mesa de Seguridad es el Asesor de Estrategia y Seguridad del Despacho de la Dirección General, como delegado del Comité Institucional de Gestión y Desempeño o quien haga sus veces, y será el encargado de coordinar las funciones de la respectiva mesa, asumiendo así el rol de Oficial de Seguridad de la Información

La ARN destinará recursos que apoyen el desarrollo de las siguientes actividades:

- Elaborar directrices y acciones que permitan la implementación, seguimiento y mejoramiento del Sistema de Gestión de Seguridad de la

Información en el marco del Sistema Integrado de Gestión para la Reintegración SIGER.

- Revisar y proponer cambios sobre el Sistema de Gestión de la Seguridad y las funciones generales en materia de seguridad y protección de la información.
- Coordinar e informar la Identificación de los riesgos, amenazas o vulnerabilidades en los activos de información y monitorear cambios significativos sobre los mismos que afecten los recursos de información frente a las amenazas más importantes.
- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
- Promover la difusión y apoyo de la seguridad de la información dentro de la ARN.
- Coordinar el proceso de administración de la continuidad de la operación de los sistemas de tratamiento de la información de la ARN frente a interrupciones imprevistas.

Responsable de Seguridad Informática:

El responsable de seguridad informática es un profesional del Grupo de Infraestructura y Soporte. Es el encargado de gestionar los sistemas de seguridad informática además de liderar la investigación y monitoreo de los incidentes relativos a la Seguridad de la Información a nivel informático.

La ARN brindará recursos para que el Oficial de Seguridad Informática pueda desarrollar las responsabilidades a su cargo:

Las responsabilidades del Oficial de Seguridad Informática son:

- Coordinar la implementación de herramientas y controles de Seguridad a nivel Informático.
- Mantener las reglas de acceso a los datos y otros recursos de TI.
- Mantener las plataformas tecnológicas de seguridad, monitoreo de tráfico, acceso y gestión de eventos de seguridad de la ARN.
- Monitorear las violaciones de seguridad y aplicar acciones correctivas para asegurar que se provea la seguridad adecuada.
- Revisar y evaluar periódicamente la política de seguridad y sugerir a la Mesa de Seguridad los cambios necesarios.
- Preparar y monitorear el programa de sensibilización en seguridad informática para todos los colaboradores.

- Probar la arquitectura de seguridad para evaluar la fortaleza de la seguridad y para detectar las posibles amenazas.
- Trabajar con la Jefatura y los Coordinadores de los Grupos de la Oficina de Tecnologías para asegurar que la seguridad esté diseñada de manera apropiada y actualizada sobre la base de retroalimentación de auditoría o de pruebas.
- Apoyar la revisión de productos y servicios en todas sus etapas desde su creación, puesta en operación y salida a producción en temas de seguridad.
- Realizar las recomendaciones, monitorear y verificar su aplicación.

Roles y Responsabilidades para los sistemas de información, aplicativos, portales y/o servicios de Tecnologías de la Información:

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

La Oficina de Tecnologías de la Información vela por la correcta utilización de todos los recursos tecnológicos y comunicaciones de la Agencia para la Reincorporación y la Normalización, como son: equipos de cómputo, sistemas de información, redes, procesamiento de datos e información y canales de comunicación.

La Oficina de Tecnologías de la Información como administradora de la infraestructura tecnológica, promulga por la adecuada gestión de la seguridad de la información procesada y/o albergada por los sistemas y servicios.

Para todo lo anterior, esta dependencia contará con el aval de la Mesa de Seguridad, así como con el compromiso de todos los colaboradores de la Entidad.

PERSONAL DIRECTIVO DE LA AGENCIA PARA LA REINCORPORACIÓN Y LA NORMALIZACIÓN

El Señor Director General, Secretario General, Director Programático de Reintegración, Jefe Oficina Asesora de Planeación, Asesor Jurídico, Jefe Oficina Asesora de Comunicaciones, Jefe Oficina de Tecnologías de la Información y Responsables de dependencias deben conocer y promulgar la existencia del Sistema de Gestión de Seguridad de la Información en la ARN, promoviendo su cumplimiento entre los colaboradores a su cargo, para que toda la entidad esté alineada con los objetivos del SGSI.

COLABORADORES DE LA AGENCIA PARA LA REINCORPORACIÓN Y LA NORMALIZACIÓN

Los colaboradores de la Agencia para la Reincorporación y la Normalización, sin importar su tipo de vinculación, son responsables de conocer, aplicar y dar estricto cumplimiento a las políticas, normas y procedimientos de la Entidad, en materia de seguridad de la información.

Todos los colaboradores de la ARN son responsables de la protección de la información de la entidad la cual acceden y/o procesan, así como de evitar su pérdida, alteración, destrucción y/o uso indebido, además de reportar los Incidentes de Seguridad informática, eventos sospechosos y el mal uso de los recursos que identifique. En cumplimiento a lo anterior los funcionarios deben firmar el documento “ACTA DE COMPROMISO Y AUTORIZACIÓN SOBRE CONFIDENCIALIDAD Y MANEJO DE LA INFORMACIÓN”.

PROPIETARIO DE LOS ACTIVOS DE INFORMACIÓN

Es el colaborador o dependencia de la Entidad a la cual, se le ha asignado la responsabilidad formal sobre un activo de información.

Sus principales responsabilidades son:

- Cumplir con la política de seguridad de la información aprobada por la Alta Dirección.
- Identificar, establecer el alcance y el valor o criticidad de los activos de información de los cuales es propietario.
- Clasificar los activos de información siguiendo la metodología de identificación y clasificación de activos aprobada.
- Identificar, definir y evaluar los riesgos a los que pudieran estar expuestos los activos de información de los cuales es propietario.
- Definir los requerimientos de seguridad de los activos de información en relación con su confidencialidad, integridad y disponibilidad.
- Informar los requerimientos y controles requeridos por los activos de información a los custodios y usuarios de los activos de información.
- Efectuar una verificación periódica de la correcta ejecución de los controles requeridos sobre los activos de información bajo su responsabilidad.

CUSTODIO DE LOS ACTIVOS DE INFORMACIÓN

Es el colaborador o dependencia de la Entidad responsable de administrar y hacer efectivos los controles que el propietario del activo de información haya definido. Sus principales responsabilidades son:

- Implementar y mantener los controles requeridos en los lugares donde estén almacenados los activos de información que se encuentren a su cargo.
- Administrar los recursos donde residen los activos de información dando los permisos definidos por el propietario del activo a los usuarios interesados.
- Proteger los activos de información presentes en los contenedores a su cargo en la situación que corresponda: almacenamiento, transporte y procesamiento.

DUEÑO DE PROCESOS

Es el colaborador o dependencia de la Entidad a la cual se le ha asignado la responsabilidad formal sobre un proceso de la entidad. Sus principales responsabilidades son:

- Apoyar la identificación de los activos de información que intervienen en el proceso correspondiente.
- Validar los activos de información identificados junto con las características básicas de cada uno de ellos.
- Apoyar y validar la identificación y designación de los propietarios de los activos de información de su proceso.

PERSONAL CON PERFIL DE USUARIO

Todos los usuarios de la Entidad sólo pueden acceder a aquellos sistemas de información a los que estén autorizados y que sean necesarios para el desempeño de sus actividades, cumpliendo con las siguientes responsabilidades:

- Resguardar la confidencialidad de la información a la tiene acceso, incluso después de haber finalizado la relación laboral con la ARN cualquiera que fuese la modalidad de vinculación con la Entidad.
- Conocer y cumplir con el Manual del Sistema de Gestión de Seguridad de la Información emitido por la entidad, procedimientos e instructivos internos, en cuestión de seguridad de la información.
- Conocer las responsabilidades y asumir consecuencias disciplinarias en caso de incurrir en el incumplimiento de alguna de las normas estipuladas en el Sistema de Gestión de Seguridad de la Información.
- Acatar procedimientos, mecanismos y medidas de seguridad, evitando cualquier intento de acceso no autorizado a recursos no permitidos.

- Usar de forma adecuada los Sistemas de información con sus respectivos procedimientos, mecanismos, controles de identificación y autentificación.
- Utilizar las contraseñas de forma adecuada, no compartirlas ni entregarlas a otros colaboradores y terceros, son de carácter personal y con uso exclusivo.
- Si un colaborador tiene sospechas de que su acceso autorizado ha sido vulnerado o está siendo utilizado por otra persona, debe iniciar el cambio de contraseña y comunicar incidencia de seguridad de la información a la Mesa de Servicios.
- Los colaboradores deben notificar al Responsable de Seguridad de la información de la Agencia para la Reincorporación y la Normalización las incidencias que detecten y afecten o pueda afectar a la información de la entidad.

PERSONAL CON ACCESO PRIVILEGIADO

Los colaboradores con acceso privilegiado y personal técnico de la entidad o de terceros, deben cumplir con las responsabilidades del personal con perfil de usuario, teniendo mayor reserva al tener acceso, realizar cambios y ajustes a la infraestructura tecnológica y sistemas de información. Todos los privilegios deben ser autorizados por el jefe inmediato del colaborador.

Las responsabilidades específicas del personal técnico y con acceso privilegiado son:

- Cumplir con las políticas y lineamientos vigentes de seguridad de la información durante la utilización de todos los sistemas de información de la Agencia para la Reincorporación y la Normalización.
- Salvaguardar toda la información almacenada en los sistemas de información.
- Gestionar todos los accesos a los usuarios, a los datos y recursos tecnológicos autorizados para la ejecución de sus actividades.
- Hacer un uso ético y responsable del acceso a la información, dados los privilegios, cumpliendo lo establecido en la normatividad del Sistema de Gestión de Seguridad de la Información.
- Guardar con medidas rigurosas las contraseñas que tienen acceso a sistemas de información con privilegios de administrador.
- Informar todas las incidencias de seguridad de la información ante cualquier violación de las normas del Sistema de Gestión de Seguridad de la Información.

- No comunicar a terceros las posibles debilidades que en materia de seguridad de los sistemas de información de la Agencia para la Reincorporación y la Normalización.

Líder o administrador funcional: es el funcionario o encargado de administrar un Sistema de Información, o Aplicativo o portal o servicio desde el punto de vista funcional. Este rol tendrá acceso a todos los sistemas de Información necesarios para desarrollar sus actividades y solucionar los problemas que se presenten.

Líder técnico: Es el funcionario o encargado de apoyar al líder o administrador funcional en aspectos técnicos de un Sistema de Información, o Aplicativo o portal o servicio desde el punto de vista técnico. Son los responsables de realizar las actividades limitadas dentro de todos los sistemas de información de la Agencia para la Reincorporación y la Normalización, estará bajo la vigilancia de los líderes o administradores funcionales y utilizan las herramientas de gestión disponibles y autorizadas por la ARN.

Dueño de servicio: Es el encargado desde el punto de vista de servicio tecnológico para gestionar los servicios a su cargo (planeación, diseño, operación, mantenimiento, monitoreo y acciones de mejora).
Administrador de Bases de Datos de la ARN: Es el funcionario encargado de la gestión de las bases de datos de la ARN.

Personal de Mesa de Servicios y Mantenimiento de los sistemas de información, aplicaciones o portales

Son los responsables de la solución de incidentes de hardware y software y en relación con sus funciones tendrán accesos privilegiados, pero no pueden acceder a archivos que contengan datos personales, con excepción de que se requiera específicamente en la gestión a desarrollar.

- La Dirección General coordina y articula el tema de seguridad física, de infraestructura, de la información, y del Talento Humano de la entidad. Así mismo la seguridad e integridad de las personas objeto de atención.
- La Dirección Programática está encargada de coordinar con las autoridades competentes las solicitudes relacionadas en temas de seguridad de las personas objeto de atención.
- La Secretaría General está encargada de la seguridad física, del talento humano y de infraestructura de la ARN.

- La Subdirección Administrativa estará a cargo del cumplimiento de la normatividad de Archivo y Plan de Preservación y Conservación de la información física.
- La Oficina de Tecnologías de la Información con el apoyo de la Subdirección Administrativa deben elaborar el Plan de Preservación Digital
- La Oficina de Tecnologías de la Información está encargada de la seguridad informática de la ARN.

III. POLÍTICAS

3.1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Agencia para la Reincorporación y la Normalización reconoce la importancia de identificar y proteger sus activos de información, la ARN está comprometida con la preservación de la confidencialidad, integridad, disponibilidad, legalidad y no repudio de toda información relacionada con su estrategia, gestión, bases de conocimiento, y otros conceptos; comprometiéndose a desarrollar, implantar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI).

De igual manera, la ARN tiene un compromiso con la seguridad de la información a través de la implantación de un conjunto adecuado de controles, tales como: políticas, prácticas, procedimientos, estructuras organizativas y funciones tecnológicas, dichos controles establecidos permiten asegurar que se cumplen los objetivos de seguridad de la información de la Entidad.

3.2. OBJETIVOS DE SGSI

- Garantizar la continuidad de los servicios de gestión de la Entidad y tecnología de la información frente a incidentes.
- Fortalecer en los colaboradores de la Agencia para la Reincorporación y la Normalización las buenas prácticas y comportamientos seguros en el manejo de información.
- Gestionar los riesgos de seguridad de la información, para que sean conocidos y según su impacto sean atendidos de una forma documentada, repetible, eficiente y adaptada al entorno y la tecnología.
- Proteger la información de la gestión y la tecnología utilizada para su procesamiento de la Agencia para la Reincorporación y la Normalización, asegurando el cumplimiento de los principios de confidencialidad, integridad y disponibilidad de la información.

3.3. CIBERDEFENSA Y CIBERSEGURIDAD EN LA ARN

En la ARN se dará cumplimiento a todo lo referente con la Ciberdefensa y Ciberseguridad del Estado Colombiano en coordinación con los entes responsables de esta labor.

Cualquier evento relacionado con: ataque cibernético, cibercrimen, ciberlavado, ciberespionaje y ciberterrorismo, debe ser atendido según los protocolos

establecidos por los entes nacionales encargados de estos temas y es el Oficial de Seguridad de la Información de la ARN quien está a cargo de establecer el procedimiento a seguir para informar al Colcert, CSIRT, entre otros; y atender los eventos con el apoyo de la Secretaría General, la Oficina Asesora Jurídica, la Oficina de Tecnologías de la Información, la Oficina de Control Interno de Gestión, y Control Interno Disciplinario.

3.4. GESTIÓN DEL RIESGO DE SEGURIDAD DIGITAL

La ARN propende por el uso responsable del entorno digital teniendo en cuenta las directrices del CONPES 3854 DE 2016, con el fin de fortalecer las capacidades para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital y los riesgos cibernéticos relacionados con el objeto misional de la Agencia.

La gestión de riesgos de seguridad digital es una herramienta enfocada a la prevención de situaciones o ataques que puedan afectar la Seguridad de la información de la ARN tales como: gusanos, ingeniería social, keyloggers, phishing, ransonware, spamming, sniffers, spoofing, o troyanos. Esta labor está a cargo del Oficial de Seguridad Informático del Grupo de Infraestructura y Soporte.

3.5. POLÍTICAS DE PLANEACIÓN ESTRATÉGICA DE TECNOLOGÍAS DE LA INFORMACIÓN

3.5.1. De la Planeación Estratégica de Tecnologías de la Información alineada con la Planeación Estratégica Institucional

La Planeación Estratégica de Tecnologías de la Información está incorporada a la Planeación Estratégica Institucional, de acuerdo con las necesidades de la entidad y la priorización en la asignación de recursos. Para lograr este objetivo, se trabaja en coordinación con la Oficina Asesora de Planeación y la Oficina de Tecnologías de la Información, en concordancia con la normatividad legal vigente.

3.5.2. De los Proyectos y Adquisición de bienes o servicios

En la elaboración de los proyectos y actividades que contengan componentes de tecnologías de la Información, las dependencias deben contar con el apoyo de la Oficina de las Tecnologías de la Información para su formulación e incorporación en el Plan de Adquisición de bienes y servicios.

De acuerdo con lo anterior, las adquisiciones de tecnologías de la información (hardware, software, servicios, aplicativos), que se adelanten en la entidad

cumplirán con los lineamientos establecidos relacionados con la armonización de los aplicativos, la compatibilidad de estos con la infraestructura de la ARN y un soporte adecuado.

Desde la Oficina Asesora de Planeación y la Oficina de Tecnologías de la Información se promueve el esquema de trabajar por gestión de proyectos. Para la gestión de proyectos de tecnologías de la información se requiere un líder funcional que se apropie del tema y busque su mejora.

Así mismo, se cuenta con un líder técnico de la Oficina de Tecnologías de la Información para acompañamiento y apoyo de la Oficina Asesora de Planeación. Los proyectos deben hacer parte del Plan de acción institucional y el seguimiento a los mismos se realizará a través del Software administrador de la planeación y la gestión – SIGER.

Todos los requerimientos de aplicativos, sistemas y equipos informáticos deben ser solicitados a través de la Mesa de Servicios de la Oficina de Tecnologías de la Información con el aval del Jefe o quien este delegue con su correspondiente justificación para su respectiva viabilidad.

3.5.3. Gestión de los sistemas de información, aplicativos y servicios de tecnologías de la información en producción.

El objetivo es mejorar la atención a los usuarios, llevar control y aplicar buenas prácticas en los sistemas de información, aplicativos o servicios de tecnologías de la información que se encuentran en producción.

Para ello es necesario:

- Asignar un responsable líder o administrador funcional por cada Sistema de información, aplicativo o servicio que se encuentra en producción, por parte del Jefe que corresponda.
- Diseñar el Servicio por cada Sistema de información, aplicativo o servicio.
- Canalizar las solicitudes a través de la Mesa de Servicios dispuesta por la OTI.
- Se cuenta con una lista de todos los sistemas de información, aplicativos y servicios.
- Para el acceso a los sistemas de información, aplicativos o servicios, Talento Humano y el Grupo de Gestión Contractual informa novedades de ingreso, traslado, retiro, vacaciones, suspensiones, de un funcionario, contratista o pasante sobre los permisos que se pueden otorgar o modificar, para evitar que los servicios no se vean afectados.

3.6. POLÍTICA DE GESTIÓN DE ACTIVOS

El objetivo es lograr y mantener la protección adecuada de los activos de información mediante la asignación de estos a los colaboradores que deben administrarlos de acuerdo con sus roles y funciones:

- El uso de los activos de información que utiliza la ARN bien sean propios o en arriendo, deben emplearse exclusivamente con propósitos laborales.
- La ARN proporcionará a los colaboradores los equipos informáticos y los programas instalados en ellos.
- Los colaboradores deberán utilizar únicamente los programas y equipos autorizados por la Oficina de Tecnologías de la Información.
- Para los terceros se deberá establecer el manejo de los activos de la información con las dependencias responsables y los supervisores de los contratos.
- La ARN es dueña de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por los colaboradores de la ARN, derivadas del objeto del cumplimiento de funciones y/o tareas asignadas, como las necesarias para el cumplimiento del objeto del contrato.
- La ARN es propietaria de los activos de información y los administradores de estos activos son los colaboradores y terceros que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware, infraestructura o servicios de Tecnologías de la Información o de los activos físicos como documentos y bases de datos manuales.
- Los colaboradores deberán garantizar que la información de la ARN que se encuentra en el equipo asignado no se pierda.
- Cuando se trate de información clasificada o reservada deberá pedir autorización a su jefe inmediato para copiar, teniendo en cuenta la clasificación de la información de acuerdo con los niveles de seguridad establecidos por la ARN; su copia, sustracción, daño intencional o utilización para fines distintos a las labores propias de la institución, serán sancionados de acuerdo con las normas y legislación vigentes.
- Todos los colaboradores propenderán por el cumplimiento de la Ley de Protección de Datos personales, la Ley de Derechos de Autor, la Ley de Transparencia y Acceso a la Información y las normas establecidas en el Manual de Seguridad de la Información.
- Todos los colaboradores propenderán por cumplimiento del Programa de Gestión Integral de Residuos de Aparatos Eléctricos y Electrónicos- RAEE y las normas vigentes en los procesos contractuales de adquisición de bienes eléctricos y electrónicos, consumibles relacionados y la baja de dichos bienes

deben dar también cumplimiento a lo dispuesto en el documento GA-M-02 "Manual para el manejo y control administrativo de los bienes de propiedad de la entidad" que está cargo del grupo de Almacén e Inventarios.

- Para los casos relacionados con contratistas ocasionales o convenios con otras entidades, las dependencias a su cargo deben contemplar los equipos y software requeridos para el cumplimiento de sus funciones. Estos equipos deben contar con su respectivo licenciamiento y actualizaciones al día. Así mismo debe contar con un antivirus actualizado. Está prohibido el uso de software no autorizado por la Oficina de Tecnologías de la Información. En este caso en particular, se debe informar el uso del equipo a la Oficina de Tecnologías de la Información de la ARN.

La Oficina de Tecnologías de la Información efectúa la revisión de los programas utilizados en cada dependencia. La descarga, instalación o uso de aplicativos o programas informáticos no autorizados será considerado como una violación a las Políticas de Seguridad de la Información de la ARN.
En caso de ser necesario y previa autorización de la Mesa de Seguridad de la ARN, los funcionarios de la Oficina de Tecnologías de la Información de la ARN podrán acceder a revisar cualquier tipo de activo de información y material que los usuarios creen, almacenen, envíen o reciban, a través de internet o de cualquier otra red o medio, en los equipos informáticos a su cargo. Los recursos informáticos de la ARN no podrán ser utilizados, sin previa autorización escrita, para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso o cualquier otro uso que no esté autorizado.

Los activos de la ARN deben ser identificados y controlados para garantizar el uso adecuado, protección y la recuperación ante desastres.

El Grupo de Almacén e Inventarios, debe llevar y administrar el inventario valorizado de Hardware de propiedad de la ARN, discriminado por dependencias y según lo estipulado en el "Manual para el manejo y control administrativo de los bienes de propiedad de la entidad". Así mismo, el control de los equipos arrendados.

Los usuarios no deben realizar intencionalmente actos que impliquen un mal uso de los recursos tecnológicos. Estos actos incluyen, pero no se limitan a: envío de correo electrónico masivo con fines no institucionales y práctica de juegos en línea.

Los usuarios no podrán efectuar ninguna de las siguientes labores sin previa autorización de la Oficina de Tecnologías de la Información:

- Instalar software en cualquier equipo de la ARN.
- Bajar o descargar software de Internet u otro servicio en línea en cualquier equipo de la ARN.
- Modificar, revisar, transformar o adaptar cualquier software propiedad de la ARN.
- Descompilar o realizar ingeniería inversa en cualquier software de propiedad de la ARN.
- Copiar o distribuir cualquier software propiedad de la ARN.

3.6.1. Inventario de activos de información

La ARN realizará la actualización del inventario de sus activos de información mínimo una vez al año, bajo la responsabilidad de cada propietario y centralizado por la Oficina Asesora de Planeación.

La ARN es propietaria de los activos de información y los administradores de estos activos son los colaboradores de la ARN que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de tecnología de información y comunicaciones.

3.7. CLASIFICACIÓN DE LA INFORMACIÓN

La ARN clasificará la información con la participación activa de los propietarios, usuarios finales y custodios de la misma, por lo que solo el propietario tiene el conocimiento necesario para determinar el nivel de calificación que debe recibir la información.

La información que se maneja en la ARN posee diferentes niveles de criticidad en cuanto al riesgo que representa su divulgación, adulteración o indisponibilidad. Por lo anterior, se hace necesario diferenciar la información según el nivel de riesgo que genera su compromiso.

Para la clasificación de la información, la ARN adopta el siguiente modelo de clasificación, compuesto por los subsiguientes tres niveles o categorías, los cuales cubren las definiciones y conceptos de la legislación vigente y estándares internacionales (Ley 1581 de 2012 de Protección de Datos, Ley 1712 de 2014 de Transparencia y acceso a la información, ISO 27000-2013).

- **Información Pública**

Es aquella información que puede ser distribuida abiertamente al público sin que cause daño alguno a la entidad, a sus colaboradores, otras dependencias o a otras entidades. Esta categorización solo puede ser asignada por el propietario de la información.

Para Datos personales de acuerdo con la Ley 1581 de 2012, se encuentran los datos públicos. La ARN trabajará la clasificación de la información con la participación activa de los propietarios, usuarios finales y custodios de la misma, por lo que solo el propietario tiene el conocimiento necesario para determinar el nivel de calificación que debe recibir la información

- **Información Reservada**

Es aquella información que tiene establecido el carácter de “Dato Sensible”, pues afecta la intimidad de las personas y su uso indebido puede generar su discriminación. El acceso a este tipo de información, así como su almacenamiento y transmisión están restringidos solo a aquellos colaboradores que se encuentren estrictamente autorizados por el propietario de la información y su divulgación solo se podrá realizar bajo los parámetros establecidos en la ley. La clasificación de la información y su manejo para dar cumplimiento a la normatividad vigente está a cargo de los administradores funcionales de los sistemas de información o las personas encargadas de las bases de datos para su salvaguarda. Así mismo, las dependencias que gestionan los documentos físicos que contienen información sensible son las responsables de su custodia. La Oficina Asesora Jurídica apoyará este proceso de clasificación.

- **Información Confidencial o Clasificada**

Es aquella información que, con base en el análisis de riesgo, haya sido clasificada como confidencial por su carácter de restringido a un grupo de personas o área en particular, bajo el concepto de necesidad de conocer. Para su divulgación, se requiere el consentimiento del propietario de la información. También pertenece a esta categoría, la información exceptuada por daño de derechos a personas jurídicas.

La información correspondiente a procesos internos confidenciales, así como la información operativa de la Agencia y los datos clasificados como “Datos personales” de acuerdo con la Ley 1266 del 2008 y la Ley 1581 de 2012,

encontrándose datos privados, semiprivados y datos sensibles, datos personales de los niños, niñas y adolescentes.

3.8. POLÍTICA DEL USO ACEPTABLE DE LOS ACTIVOS

Todos los colaboradores que hagan uso de los activos de la ARN tienen la responsabilidad de dar cumplimiento a las siguientes reglas establecidas para el uso aceptable de los activos, entendiendo que el uso no adecuado de los recursos pone en peligro la continuidad del negocio y generar sanciones de acuerdo con las normas y legislación vigentes.

Regla 1: Del Uso del Servicio de Internet

El servicio de Internet suministrado por la Agencia para la Reincorporación y la Normalización es una herramienta de apoyo a las funciones y responsabilidades de los funcionarios, por lo tanto, su utilización debe observar y cumplir las directrices que a continuación se relacionan:

- El uso del Servicio de Internet está limitado exclusivamente para propósitos laborales.
- Los servicios a los que un determinado usuario pueda acceder desde la Internet dependerán del rol que desempeña el usuario en la ARN y para los cuales esté formal y expresamente autorizado.
- Todo usuario es responsable de informar de contenidos o acceso a servicios que no le estén autorizados y/o no correspondan a sus funciones dentro de la ARN.
- Está expresamente prohibido el envío y/o descarga y/o visualización de páginas con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor y/o que atenten contra la integridad moral de las personas o instituciones.
- Está expresamente prohibido el acceso a páginas web, portales, sitios web y/o aplicaciones web que no hayan sido autorizadas por la ARN.
- Está expresamente prohibido el envío y/o descarga de cualquier tipo de software o archivos de fuentes externas y/o de procedencia desconocida.
- Está expresamente prohibida la propagación de virus o cualquier tipo de código malicioso.
- Está expresamente prohibido acceder a páginas que agredan la ética y el buen comportamiento.

La ARN se reserva el derecho de monitorear los accesos y por tanto uso del Servicio de Internet de todos sus colaboradores, además de limitar el acceso a

determinadas páginas de Internet, los horarios de conexión, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro ajeno a los fines institucionales.

Regla 2: Del Uso de herramientas de colaboración tales como Skype Empresarial y Correo Electrónico

Dichas herramientas son para apoyo a las funciones y responsabilidades de los funcionarios de la Agencia para la Reincorporación y la Normalización, en tal virtud, su uso debe sujetarse a las siguientes directrices:

- Las herramientas de colaboración incluyen servicios tales como: correo electrónico, listas de distribución, chat, escritorio compartido, video chat, videoconferencia, llamada de voz, las cuales deben ser empleadas únicamente para temas laborales. En consecuencia, no pueden ser utilizadas con fines personales, económicos, comerciales y/o cualquier otro ajeno a los propósitos de la Entidad.
- Se debe preferir el uso del correo electrónico al envío de documentos físicos siempre que las circunstancias lo permitan, cumpliendo con los lineamientos de uso eficiente del papel.
- Está prohibido el uso de correos masivos tanto internos como externos, salvo a través del correo institucional “Somos ARN” el cuál es administrado por el grupo de comunicaciones.
- Todo mensaje SPAM o CADENA debe ser inmediatamente reportado al correo soporteacr@reincorporacion.gov.co, eliminado y nunca respondido. No está permitido el envío y/o renvío de mensajes en cadena.
- Toda actividad sospechosa respecto a la difusión de contenidos inusuales, en especial si contiene archivos adjuntos con extensiones .exe, .bat, .prg, .bak, .pif, que tengan explícitas referencias eróticas o alusiones a personajes famosos, deben ser inmediatamente reportado al correo soporteacr@reincorporacion.gov.co y posteriormente eliminado, ya que puede ser contentivo de malware.
- La cuenta de correo Institucional no debe ser revelada a páginas o sitios publicitarios, de compras, deportivos, agencias matrimoniales, casinos o a cualquier otra ajena a los fines de la ARN.
- Las listas de distribución serán solicitadas por los jefes, designando el responsable administrador de la misma para mantenerla actualizada.
- Está expresamente prohibido el uso de las herramientas de colaboración para la transferencia de contenidos insultantes, ofensivos, injuriosos, obscenos, violatorios de los derechos de autor y/o que atenten contra la integridad moral de las personas o instituciones.

- Está expresamente prohibida la propagación de virus o cualquier tipo de código malicioso a través de las herramientas de colaboración.
- Todos los correos electrónicos corporativos con destino externo deben contener una sentencia de confidencialidad con un contenido como el siguiente:
  "…El presente mensaje, incluyendo sus archivos adjuntos, es para el uso exclusivo de la(s) persona(s) o entidad(es) a quien(es) fue dirigido y puede contener información de carácter RESERVADA, CONFIDENCIAL y/o LEGALMENTE PROTEGIDA. En consecuencia, el uso, divulgación, reproducción total y/o parcial o cualquier otra utilización de la información aquí contenida está prohibida. Si usted recibe este mensaje por error, le solicitamos notificar inmediatamente al emisor y eliminar esta comunicación y todas sus copias…".
- Las únicas herramientas de colaboración (Correo electrónico, Chat, videochat, reuniones virtuales, llamadas por voz y escritorio compartido) autorizadas en la entidad son las asignadas por la Oficina de Tecnologías de la Información, las cuales cumplen con todos los requerimientos técnicos, de seguridad y licenciamiento, evitando ataques de virus, spyware y otros tipos de software malicioso. Además, estos servicios tienen respaldo de diferentes procesos de copia de respaldo (backup) aplicados de manera periódica y segura.

- La ARN puede supervisar cualquier sesión, llamada o cuenta de correo para certificar que se está usando para los propósitos legítimos. El incumplimiento de esta política puede conducir a acciones disciplinarias tales como terminación de la relación laboral o acciones de índole legal.

Regla 3: Del Uso de los Recursos Tecnológicos

Los recursos tecnológicos de la Agencia para la Reincorporación y la Normalización son herramientas de apoyo a las labores y responsabilidades de los colaboradores; por ello, su uso está sujeto a las siguientes directrices:

- Los bienes de cómputo se emplean de manera exclusiva y bajo la completa responsabilidad del colaborador al cual han sido asignados y únicamente para el correcto desempeño de las funciones del cargo, por lo tanto, no pueden ser utilizados con fines personales o por terceros no autorizados.
- Las impresoras de red son recursos tecnológicos compartidos por lo cual su uso debe ser moderado y su mantenimiento será realizado estrictamente por los colaboradores de la Oficina de Tecnologías de la Información. La impresión de documentos deberá ajustarse a la política de uso eficiente del papel de la entidad a cargo de Secretaría General.

- Los usuarios no deben mantener almacenados en los discos duros, de las estaciones cliente o discos virtuales de red, archivos de video, música y fotos que no sean de carácter institucional.
- Es responsabilidad del colaborador velar por la conservación y cuidado de los activos a su cargo evitando fumar, ingerir alimentos o bebidas en el área de trabajo donde se encuentren elementos tecnológicos.
- No está permitido realizar derivaciones eléctricas desde las fuentes de corriente regulada ni conectar multi-tomas a las mismas. Sobre los equipos tecnológicos no deben ubicarse elementos pesados, radios de comunicación o teléfonos celulares.
- Las únicas personas autorizadas para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos como destapar, agregar, desconectar, retirar, revisar y/o reparar sus componentes, son los colaboradores de la Oficina de Tecnologías de la Información o quienes sean designados por ellos para tal labor.
- Toda unidad de almacenamiento externo como CDs, DVDs, memorias USB o Discos Duros externos debe ser verificada por el programa antivirus licenciado y autorizado por la OTI, previo a su ingreso a los recursos de cómputo de la entidad.
- La única dependencia autorizada para trasladar los elementos y/o recursos tecnológicos de un puesto de trabajo a otro es el Grupo de Almacén e Inventarios. En tal virtud, esta función debe ajustarse a los procedimientos y competencias de esta dependencia.
- Toda asignación y reasignación de los equipos de cómputo será realizada por la Oficina de Tecnologías de la Información y en concordancia a los procedimientos y competencias de esta dependencia.
- El retiro de recursos tecnológicos de la entidad solo está permitido, previa autorización de la Subdirección Administrativa de acuerdo con el procedimiento establecido por esa dependencia.
- La pérdida o daño de elementos o recursos tecnológicos o de alguno de sus componentes debe ser informada de inmediato a la Subdirección Administrativa por el colaborador a quien se le hubiere asignado.
- Todo problema de orden técnico con los equipos tecnológicos debe ser reportado mediante el procedimiento establecido por la Oficina de Tecnologías de la Información a la mayor brevedad posible.
- Solo está permitido el uso de software licenciado por la Entidad y/o aquel que sin requerir licencia sea expresamente autorizado por la Oficina de Tecnologías de la Información.
- Los únicos autorizados para instalar y/o desinstalar programas o herramientas de software son los colaboradores de la Oficina de Tecnologías de la

Información. Está expresamente prohibido instalar, ejecutar y/o utilizar programas o herramientas de software o hardware no autorizadas por la OTI.

- La Oficina de Tecnologías de la Información es la única dependencia autorizada para realizar copias del software licenciado por la Entidad, el cual no debe ser copiado, suministrado a terceros o utilizado para fines personales.
- Todo acceso a la red de la Entidad mediante elementos o recursos tecnológicos no institucionales deberá ser informado, autorizado y controlado por la Oficina de Tecnologías de la Información.

Regla 4: Del Manejo de la Información

- La copia de información RESERVADA o CONFIDENCIAL deberá ser autorizada por el Propietario de la información.
- La información RESERVADA solo podrá ser almacenada en las bases de datos de los sistemas de información dispuestos para este fin, para garantizar su seguridad y respaldo.
- La información CONFIDENCIAL deberá ser almacenada en los discos de red en las carpetas indicadas con el fin de garantizar su seguridad y respaldo. En ningún caso deberá realizarse en el disco duro u otro componente del computador personal.
- El acceso a la información RESERVADA y/o CONFIDENCIAL solo podrá ser autorizado por el propietario de la información.
- Los acuerdos de No-Divulgación de Información que se suscriban con terceros deberán incluir cláusulas referentes al uso de la información y su destrucción posterior.
- Está expresamente prohibido distribuir información de la ARN, no pública, a otras entidades o ciudadanos sin la debida autorización.
- Está prohibido utilizar medios de almacenamiento externo que no sean propiedad de la ARN, para tomar copias de seguridad de la información, sin previa autorización del Jefe correspondiente.
- Talento Humano se encargará de tramitar la firma de Acuerdo de Tratamiento de Datos Personales de los funcionarios de la ARN y que repose una copia en su hoja de vida.
- El Grupo de Gestión Contractual se encargará de tramitar la firma de Acuerdo de Tratamiento de Datos Personales de los contratistas de prestación de servicios de la ARN y que repose una copia en su carpeta de contrato.
- El Grupo de Gestión Contractual se encargará de tramitar solicitud de información de contratistas (Personas jurídicas), que realizan tratamiento de datos personales cuya responsabilidad es de la ARN, sobre el cumplimiento de la Ley de Protección de Datos Personales y sus decretos reglamentarios y deberá reposar copia en la carpeta contractual.

3.9. POLÍTICA DE INTERCAMBIO DE INFORMACIÓN

La ARN propende por la protección de la información en el momento en que sea transferida o intercambiada con otras entidades y establece los procedimientos y controles necesarios para el intercambio de información; así mismo, se establecen Acuerdos de Confidencialidad y/o de Intercambio de Información con las terceras partes con quienes se realice dicho intercambio.

La ARN propende por el uso de tecnologías informáticas para llevar a cabo el intercambio de información digital y establece directrices para el intercambio de información en medio físico.

Normas de intercambio de información

- El Grupo de Gestión Contractual, en acompañamiento con la Oficina Asesora Jurídica debe definir los modelos de Acuerdos de Confidencialidad y/o de Intercambio de Información entre la Entidad y terceras partes incluyendo los compromisos adquiridos y las acciones civiles o penales por el incumplimiento de dichos acuerdos. Entre los aspectos a considerar se debe incluir la prohibición de divulgar la información entregada por la ARN a los terceros con quienes se establecen estos acuerdos y la destrucción de dicha información una vez cumpla su cometido.
- El Grupo de Gestión Contractual debe establecer en los contratos que se suscriban con terceras partes, los Acuerdos de Confidencialidad o Acuerdos de intercambio dejando explícitas las responsabilidades y obligaciones legales asignadas a dichos terceros por la divulgación no autorizada de información que les ha sido entregada debido al cumplimiento de los objetivos misionales de la ARN.
- La Oficina de Tecnologías de la Información a través del Profesional Especializado de Seguridad Informática debe definir y establecer el mecanismo de intercambio de información digital con los diferentes terceros que hacen parte de la operación de la ARN, que reciben o envían información de las personas objeto de atención de la ARN, el cual contemple la utilización de medios de transmisión confiables y la adopción de controles, con el fin de proteger la confidencialidad e integridad de la misma.
- Los supervisores de convenios y contratos deben velar porque el intercambio de información de la ARN con entidades externas se realice en cumplimiento de las Políticas de seguridad para el intercambio de información aquí descritas, los Acuerdos de Intercambio de Información y los mecanismos definidos para dicho intercambio de información.

- Los propietarios de los activos de información deben asegurar que los datos requeridos sólo puedan ser entregados a terceros, previo consentimiento de los titulares de los mismos, salvo en los casos que lo disponga una ley o sea una solicitud de los entes de control.
- Los propietarios de los activos de información, o a quien ellos deleguen, deben verificar que el intercambio de información con terceros deje registro del tipo de información intercambiada, el emisor y receptor de la misma y las fechas de entrega/recepción.
- Los propietarios de los activos de información deben autorizar los requerimientos de solicitud o envío de información de la ARN a terceras partes, salvo que se trate de solicitudes de entes de control o de cumplimiento de la legislación vigente.
- Los propietarios de los activos de información deben asegurarse que el Intercambio de información digital solamente se realice si se encuentra autorizada y dando cumplimiento a las Políticas de administración de redes, de acceso lógico y de protección de datos personales de la ARN, así como del mecanismo de intercambio de información.
- Los terceros con quienes se intercambia información deben destruir de manera segura la información suministrada, una vez esta cumpla con la función para la cual fue enviada y demostrar la realización de las actividades de destrucción.
- Los terceros con quienes se intercambia información de la ARN deben darle manejo adecuado a la información recibida, en cumplimiento de las Políticas de seguridad de la Entidad, de las condiciones contractuales establecidas y del documento de intercambio de información.
- Los usuarios deben propender por el uso de las carpetas compartidas para el manejo de información sensible, siguiendo las políticas de seguridad de la información establecidas. No deben utilizar el correo electrónico personal como medio para enviar o recibir información sensible de la ARN.
- No está permitido el intercambio de información sensible de la ARN por vía telefónica.

3.10. POLÍTICA DE LA SEGURIDAD DE LOS RECURSOS HUMANOS

La Agencia establece las siguientes directrices que se deben cumplir en los procesos de selección, permanencia y desvinculación de los colaboradores de la ARN, con el objetivo de reducir los riesgos generados por el error humano, comisión de ilícitos, uso inadecuado de los recursos y manejo inapropiado de la información.

- Como parte de las condiciones iniciales de ingreso, todos los colaboradores firmarán un compromiso de confidencialidad de la información, a través del

documento “ACTA DE COMPROMISO Y AUTORIZACIÓN SOBRE CONFIDENCIALIDAD Y MANEJO DE LA INFORMACIÓN”.

- Todos los colaboradores deben contar con una inducción respecto de las Políticas de Seguridad de la Información, la cual debe ser realizada por el responsable del SGSI o a quien este delegue.
- Todos los productos, creaciones, desarrollos, campañas, trabajos, investigaciones, etc., en el desarrollo de sus funciones, logrados por un colaborador durante la vigencia de su vinculación, serán propiedad de la ARN.
- Es responsabilidad de cada colaborador conocer y dar cumplimiento de las Políticas de Seguridad de la Información, así como, asistir a las charlas o entrenamientos dispuestos para tal fin.
- En caso de presentarse una situación administrativa con el recurso humano de una dependencia que pueda alterar la prestación de los servicios, el jefe de esta debe tramitar los permisos para el (los) funcionario(s) delegado(s) en los sistemas de información correspondientes a través de la mesa de ayuda.

3.11. POLÍTICA DE GESTIÓN DE COMUNICACIONES Y OPERACIONES

Establecer responsabilidades y procedimientos para la gestión y operación de los recursos de procesamiento de la información y las comunicaciones, para garantizar su funcionamiento correcto y seguro.

3.11.1. Protección contra Código Malicioso

Todas las estaciones de trabajo de la ARN deben contar con su respectivo software de detección y reparación de códigos maliciosos para la verificación de los sistemas según el siguiente esquema:

- Verificar en tiempo real, la presencia de códigos maliciosos en archivos de medios de almacenamiento masivo extraíbles o en archivos recibidos a través de la red.
- Desplegar tareas de escaneo diario en busca de códigos maliciosos en todas las unidades de almacenamiento de la estación de trabajo.
- La actualización de la base de datos de detección debe ser mínimo de una vez por día. Adicionalmente se deberá tener en cuenta las siguientes disposiciones:
  - Se debe contar con verificación de las páginas web para comprobar la presencia de códigos maliciosos.
  - Ningún colaborador podrá ejercer actividades de administración sobre su equipo. Los únicos autorizados para desarrollar esta función son los colaboradores de la Oficina de Tecnologías de la Información o a quién ellos designen.

- Se prohíbe estrictamente el uso de software no autorizado.
- La Oficina de Tecnologías de la Información realizará sensibilización al personal sobre la protección contra software malicioso y buenas prácticas de seguridad informática.

3.11.2. Respaldo de la Información

Se deben realizar y mantener copias de seguridad de la información de la entidad con el objetivo de recuperar los Sistemas de información en caso de cualquier tipo de falla, ya sea de hardware, software o de procedimientos operativos al interior de la entidad.

La Oficina de Tecnologías de la Información efectuará copias de la Información contenida en los Sistemas de Información de acuerdo con el siguiente esquema:

- Backup Mensual: Corresponde a la copia mensual completa en cinta de la información y el resultado se registra a través de la herramienta de automatización de la tarea. La copia se realiza los últimos diez (10) días hábiles de cada mes.

- Backup Semanal: Corresponde a la copia semanal completa en cinta de la información y el resultado se registra a través de la herramienta de automatización de la tarea. La copia se realiza entre sábado y domingo de cada semana según programación.

- Backup Diario/Incremental: Corresponde a la copia diaria incremental en disco de la información y el resultado se registra a través de la herramienta de automatización de la tarea. La copia se realiza en horario no hábil según programación.

Adicionalmente, se tendrán en cuenta las siguientes disposiciones:

- Se debe realizar backups como mínimo, en los servidores donde operan los ambientes de producción del sistema misional.
- Los medios de almacenamiento sobre los cuales residen los backups, deben tener una vida útil de mínimo tres años a partir de su ejecución.
- Los backups deben almacenarse en un lugar seguro, con las condiciones de temperatura y humedad requerida, para su adecuada conservación y durabilidad.
- Los medios magnéticos y/o ópticos donde residen los backups, deben estar debidamente etiquetados y ordenados.

- El acceso al lugar de almacenamiento debe ser restringido y solo podrá hacerse mediante autorización del Coordinador del Grupo de Infraestructura y Soporte o a quién él designe.
- Los backups de los sistemas centralizados son responsabilidad del Grupo de Infraestructura y Soporte y solo deben ser realizados por los colaboradores de dicho grupo.
- El grupo de Infraestructura y Soporte debe contar con el respectivo documento de restauración de backups de tal forma que permita recuperar los ambientes de trabajo requeridos en tiempos razonables.
- Los backups no generados en los esquemas mencionados para el respaldo de la información, se obtendrán del backup mensual o en su defecto del último respaldo realizado.

3.11.3. Gestión de seguridad en redes

- Se deben implementar controles de seguridad basados en las capas de red, con el fin de garantizar una interconexión fácil y eficiente, a la vez que se proteja la información y los recursos computacionales de la entidad.
- Toda actividad en la red deberá ser registrada y monitoreada a fin de detectar y controlar situaciones anómalas.
- Se debe implementar la independencia de la red de colaboradores y la de invitados.

3.12. POLÍTICA DE CONTROL DE ACCESO

Establecer los lineamientos que permitan prevenir el acceso no autorizado a los sistemas de información, bases de datos y sistemas de procesamiento de la información de la ARN.

3.12.1. De los Centros de Procesamiento de Datos

El acceso a los centros de datos debe ser debidamente controlado para lo que se dictan las siguientes disposiciones:

- Solo se permite el ingreso al centro de datos de personal que esté expresamente autorizado.
- Los accesos a los centros de datos por parte del personal autorizado deben requerir de un método de identificación del colaborador para conceder el acceso y debe quedar registrado detallando nombre, fecha y hora, tanto del ingreso como del egreso.

- Las visitas a los centros de datos deben estar expresamente autorizadas por el Coordinador de Infraestructura y Soporte y debe quedar registro detallando nombre, fecha y hora, tanto del ingreso como del egreso, del visitante. Durante la permanencia, debe siempre estar acompañado de personal autorizado.
- Cuando un colaborador finaliza su relación laboral, sus permisos de acceso deberán ser revocados de forma inmediata.
- El coordinador de Infraestructura y Soporte o a quién él delegue es el responsable de asignar los permisos de acceso a los centros de datos según lo considere necesario.
- Todo ingreso o retiro de algún equipo de computación o comunicaciones de los centros de datos, debe ser autorizado por el Coordinador de Infraestructura y Soporte.

3.12.2. De los Sistemas de Información

Para adquisiciones de aplicativos de terceros o desarrollos propios las dependencias deberán atender los lineamientos de la Oficina de Tecnologías de la Información e informar sobre la necesidad para trabajar en forma conjunta la solución.

3.12.3. Credenciales de Acceso

- Las credenciales de acceso a la red y/o recursos informáticos (Usuario y Clave) son de carácter estrictamente personal e intransferible, los colaboradores no deben revelar estas a terceros ni utilizar claves ajenas.
- Todo colaborador es responsable de los registros y/o modificaciones de información que se hagan a nombre de su cuenta de usuario, toda vez que la clave de acceso es de carácter personal e intransferible.
- Todas las contraseñas deben tener una longitud mínima de OCHO (8) caracteres que deben cumplir con las siguientes características: Incluir combinación de números, letras mayúsculas, letras minúsculas y caracteres especiales.
- Después de cinco (5) intentos de acceso fallidos de manera consecutiva por ingreso de usuario y/o contraseña errados, el usuario será bloqueado hasta nueva reactivación por parte del administrador.
- Las contraseñas de acceso a los sistemas de información deben ser cambiadas periódicamente, de igual forma cualquier cambio extemporáneo de contraseña solamente puede ser solicitado por el titular de la cuenta o su jefe inmediato.

- Cuando un colaborador se retira de la ARN, todas las credenciales asignadas sobre los recursos informáticos otorgados deben ser inhabilitadas inmediatamente.
- Las cuentas de usuario en estado deshabilitado que cumplan un periodo de tres meses en dicho estado deberán ser eliminadas.
- Los usuarios y contraseñas de servicio al igual que los requeridos para interacción entre aplicaciones y otros sistemas de información no deben estar embebidos explícitamente dentro del código fuente del software.
- Las credenciales de acceso a los sistemas de información críticos de la entidad con privilegios de administración deben cumplir con los lineamientos de custodia definidos por la Oficina de Tecnologías de la información con el fin de garantizar la confidencialidad y disponibilidad de la información.
- No se deben mantener listados de contraseñas en archivos de ningún tipo expuestos en servidores o medios de almacenamiento que puedan ser vulnerados o accedidos por usuarios no autorizados.
- La Oficina Asesora Jurídica apoyará el registro de los Derechos de Autor cuando corresponda.
- Los responsables de los servicios deberán atender el plan de preservación digital.

3.12.4. Estaciones de Trabajo

Todas las estaciones de trabajo deben tener una contraseña de ingreso y un protector de pantalla con contraseña y activación automática luego de un periodo de tiempo definido.

- En ausencia del colaborador, el acceso a la estación de trabajo debe ser bloqueado, de lo contrario se expone la información y el acceso a terceros no autorizados, que puedan generar daño, alteración o uso indebido, así como a la suplantación del usuario original.
- Todos los colaboradores de la Entidad deben revisar, e investigar los derechos de propiedad intelectual para todo material como libros, artículos, informes, imágenes, software y/o sitios Web encontrados en Internet antes de ser usados para cualquier propósito con el fin de asegurar el cumplimiento de la legislación vigente.
- La conexión remota a la red interna de la ARN debe ser realizada exclusivamente a través del servicio de acceso seguro mediante conexión VPN suministrada por la entidad.

3.13. POLÍTICA DE PANTALLA Y ESCRITORIO LIMPIO

3.13.1. Ubicación y protección de equipos de cómputo e impresoras

- El área de trabajo de los colaboradores de la ARN debe localizarse preferiblemente en instalaciones que no queden expuestas al acceso de personas externas.
- Cuando sea aplicable, en los lugares donde se almacene información sensible, se deben implementar condiciones ambientales mínimas para el resguardo de los activos de información.
- Cualquier documentación confidencial o sensible que sea reproducida en equipos multifuncionales se debe retirar inmediatamente del equipo

3.13.2. Equipo desatendido por el colaborador

- Toda vez que el colaborador se ausente de su lugar de trabajo debe bloquear su equipo de cómputo con el fin de no permitir el acceso a las aplicaciones o servicios de la Entidad, además debe guardar en lugar seguro cualquier documento o medio magnético que contenga información confidencial y gestionar su entrega lo antes posible a Gestión Documental.
- La pantalla de autenticación a la red de la Entidad debe requerir solamente la identificación de la cuenta y una clave y no entregar o solicitar otra información.
- La autenticación del usuario debe ser requerida cada vez que el equipo se encienda, reinicie, bloquee o después de aparecer el protector de pantalla.

3.14. POLÍTICA PARA USO DE DISPOSITIVOS MÓVILES

La ARN dispondrá de dispositivos móviles para los colaboradores que por sus funciones así lo requieran. La gestión de dichos dispositivos está a cargo de la Subdirección Administrativa, quien velará porque los colaboradores hagan un uso responsable de los servicios y equipos proporcionados por la entidad, para lo cual se establecen las siguientes directrices.

- Evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.
- Evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales a los dispositivos móviles institucionales.
- Cada vez que el sistema de sus dispositivos móviles institucionales notifique de una actualización disponible, aceptar y aplicar la nueva versión.

- Evitar hacer uso de redes inalámbricas de uso público, en el mismo sentido se deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.
- Evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.
- Evitar almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.
- Evitar modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.

3.15. POLÍTICAS DE CRIPTOGRAFÍA

3.15.1. Política de controles criptográficos

La ARN velará por el fortalecimiento de la confidencialidad, disponibilidad e integridad de la información de la Entidad, clasificada como reservada, mediante el cifrado de datos durante su tratamiento.

3.15.2. Normas de controles criptográficos

- Los propietarios de los activos de información y los responsables de su tratamiento deberán almacenar y/o transmitir la información digital clasificada como reservada o restringida, bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad.
- La Oficina de Tecnologías de la Información proveerá las herramientas de encripción de datos a los usuarios, previa solicitud formal del propietario del activo de información.
- Para el caso de Sistemas de Información desarrollados internamente, la Oficina de Tecnologías de la Información evaluará la implementación de métodos para cifrar la información reservada o restringida, teniendo en cuenta el impacto que tenga respecto al rendimiento de dichos sistemas.

3.16. POLÍTICA DE RELACIÓN CON PROVEEDORES

La ARN establecerá mecanismos de control en sus relaciones con terceras partes, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por las mismas, cumplan con las políticas, normas y procedimientos de seguridad de la información.

Los Supervisores de contratos con terceros deben divulgar las políticas, normas y procedimientos de seguridad de la información de la ARN a dichos terceros, así como velar porque el acceso a la información y a los recursos de almacenamiento o procesamiento de la misma, por parte de los terceros se realice de manera segura, de acuerdo con las políticas, normas y procedimientos de seguridad de la información.

La gestión del riesgo de la entidad debe identificar y monitorear los riesgos relacionados con los contratistas o proveedores, haciendo extensiva esta actividad a la cadena de suministro de los servicios de tecnología o comunicaciones.

3.17. POLÍTICA DE GESTIÓN DE VULNERABILIDADES

La ARN, a través de la Oficina de Tecnologías de la Información verifica la existencia de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de la realización periódica de pruebas de vulnerabilidades.

3.17.1. Normas para la gestión de vulnerabilidades a través del Grupo de Infraestructura y Soporte:

- Adelantar los trámites correspondientes para la realización de pruebas de vulnerabilidades con una periodicidad establecida, por un ente independiente al área objeto de las pruebas, con el fin de garantizar la objetividad del desarrollo de las mismas.
- Revisar periódicamente la existencia de nuevas vulnerabilidades técnicas y reportarlas a los administradores de la plataforma tecnológica y los desarrolladores de los sistemas de información, con el fin de prevenir la exposición al riesgo de estos.
- Generar y ejecutar o monitorear planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica.
- Revisar, valorar y gestionar las vulnerabilidades técnicas encontradas, apoyándose en herramientas tecnológicas para su identificación.

3.18. POLÍTICA DE CONTINUIDAD DEL NEGOCIO

Es el conjunto de procedimientos y estrategias definidos para asegurar la reanudación oportuna y ordenada de los procesos del negocio generando un impacto mínimo ante una contingencia, dentro de los cuales se tiene prevenir interrupciones en las actividades de la ARN que van en detrimento de los procesos críticos de la entidad afectados por situaciones no previstas o desastres.

Teniendo en cuenta que es un tema transversal, la Dirección General de la ARN delegó a la Secretaría General a través de la Subdirección Administrativa para coordinar el diagnóstico y presentar Plan de Continuidad del Negocio (BCP).

Los responsables del BCP deben establecer los lineamientos para minimizar los efectos de las posibles interrupciones de la operación (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación, teniendo en cuenta los siguientes aspectos:

- Análisis de riesgos: Identificar los procesos críticos y riesgos asociados a la no operatividad de los mismos, así como la valoración objetiva de los riesgos y escenarios identificados, bajo criterios como criticidad de la amenaza, probabilidad de ocurrencia, entre otros.
- Análisis de impacto del negocio: Identificar los productos y servicios claves de la ARN teniendo en cuenta todos los factores que hacen parte de los mismos, tales como personal, equipos, proveedores entre otros, con el fin de valorizar el impacto que puede contraer una interrupción inesperada en las funciones diarias. Estimar los tiempos de recuperación, Identificar los requerimientos de recursos indispensables para el funcionamiento de los procesos clave.
- Selección de la estrategia de continuidad: Se definen los requerimientos, recursos y roles encargados, los procedimientos y técnicas de recuperación con base en las dos primeras fases y en los escenarios identificados.
- Ejecución y desarrollo del plan: Establecer e implementar el Plan de recuperación, actividades de capacitación y entrenamiento, pruebas de recuperación, divulgación, entre otros. Designación de responsables y asignación de recursos
- Plan de evaluación y de mantenimiento: Retroalimentación, mejora continua, plan de pruebas periódicas, simulacros y velar porque se cumpla el plan.

IV. DE LA PROTECCIÓN DE DATOS PERSONALES

4.1. POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

La ARN conforme a las disposiciones contenidas en la ley 1581 de 2012 y sus decretos reglamentarios, como custodio responsable y/o encargado del tratamiento de datos personales, propenderá por la seguridad y confidencialidad de los datos sensibles o personales que se hayan recogido y tratado en operaciones tales como la recolección, almacenamiento, uso, circulación y

supresión de aquella información que se reciba de terceros a través de los diferentes canales de recolección de información Se entiende por dato personal cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables, como el nombre, la edad, el sexo, el estado civil, el domicilio, entre otros. Esto datos pueden ser almacenados en cualquier medio físico o electrónico y ser tratados de forma manual o automatizada.

V. ASIGNACIÓN DE RESPONSABILIDADES

- **Responsable de tratamiento**: La ARN, de acuerdo con la ley de protección de datos personales es Responsable de Tratamiento de datos personales contenidos en sus bases de datos.

- **Encargado del Tratamiento**: La ARN podrá realizar el tratamiento de sus datos personales a través de encargados.

- **Administrador de base de datos personales**: Funcionario o Encargado que tiene a cargo y realiza tratamiento a una o más bases de datos que tiene información personal, bien sea automatizada o manual.

- **Gestor**: La Oficina Asesora de Planeación llevará el control del registro de las bases de datos con información personal que hay en la ARN y apoyará el ingreso de la información en el Registro Nacional de Base de Datos de la Superintendencia de Industria y Comercio.

  Así mismo, la Oficina Asesora de Planeación debe informar a la delegatura de protección de datos personales de la SIC cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares, las cuales deben ser informadas a través de correo electrónico a la Oficina Asesora de Planeación por parte de la Oficina de Tecnologías de la Información o del Grupo de Atención al Ciudadano, siendo éstas las dependencias a través de las cuales se puede realizar la identificación de dichas inconsistencias.

- **Garante**: El Grupo de Atención al Ciudadano coordinará la atención y respuesta de las peticiones, quejas, reclamos, solicitudes y denuncias relacionados con la Ley de Protección de Datos Personales que los titulares realicen a la ARN y el derecho de Habeas Data.
- **Apoyo Jurídico**: La Oficina Asesora Jurídica coordinará todos los temas jurídicos y emitirá los conceptos que faciliten el actuar de la ARN y mitiguen los

riesgos de su gestión en materia de seguridad de la información. Dentro de sus actividades está la clasificación y sub-clasificación de la información de acuerdo con las normas vigentes.

- **Control Interno disciplinario**: Control Interno Disciplinario apoyará a la alta dirección los temas relacionados con las sanciones y violaciones a las políticas de seguridad de la información en la ARN.

VI. CLASIFICACIÓN DE LA INFORMACIÓN RELACIONADA CON DATOS PERSONALES

Para el manejo de los datos personales en la ARN, se requieren incluir dentro de la clasificación de la información lo establecido en la Ley 1266 de 2008 y la Ley 1581 de 2012:

- Dato privado: “Según tipología por protección de datos personales, es el dato que por su naturaleza íntima o reservada sólo es relevante para el Titular de la información”

- Dato semiprivado: “Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su Titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios”

- Dato público: “Es el dato calificado como tal según los mandatos de la Ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados”. “Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas”.

- Datos sensibles: Son “aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos”.

  La Ley 1581 de 2012 prohíbe el tratamiento de datos sensibles con excepción de los siguientes casos: (i) cuando el Titular otorga su consentimiento, (ii) el

Tratamiento es necesario para salvaguardar el interés vital del Titular y éste se encuentre física o jurídicamente incapacitado, (iii) el tratamiento es efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad, (iv) el Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y (v) el Tratamiento tenga una finalidad histórica, estadística o científica, en este último caso deben adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

- Datos personales de los niños, niñas y adolescentes: Se debe tener en cuenta que aunque la Ley 1581 de 2012 prohíbe el tratamiento de los datos personales de los niños, niñas y adolescentes, salvo aquellos que por su naturaleza son públicos, la Corte Constitucional precisó que independientemente de la naturaleza del dato, se puede realizar el tratamiento de éstos “siempre y cuando el fin que se persiga con dicho tratamiento responda al interés superior de los niños, niñas y adolescentes y se asegure sin excepción alguna el respeto a sus derechos prevalentes”. (Fuente: Sentencia C-748/11).

VII. DISPOSICIONES GENERALES PARA LA PROTECCIÓN DE DATOS PERSONALES EN LA ARN:

- La ARN dará cumplimiento a la normatividad legal vigente que dicte disposiciones para la protección de datos personales.

- La ARN realiza el tratamiento de Datos Personales en ejercicio propio de sus funciones legales y para el efecto no requiere la autorización previa, expresa e informada del Titular. Sin embargo, cuando no corresponda a sus funciones deberá obtener la autorización por medio de un documento físico, electrónico, mensaje de datos, Internet, sitio web, o también de manera verbal o telefónica o en cualquier otro formato que permita su posterior consulta a fin de constatar de forma inequívoca que sin el consentimiento del titular los datos nunca hubieran sido capturados y almacenados en medios electrónicos o físicos. Así mismo, se podrá obtener por medio de conductas claras e inequívocas del Titular que permitan concluir de una manera razonable que este otorgó su consentimiento para el manejo de sus Datos Personales.

- La información que se publique o divulgue por cualquier medio de Internet, de cualquier colaborador de la Agencia, que sea creado a nombre personal en redes sociales, se considera fuera del alcance del SGSI y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán responsabilidad de la persona que la haya publicado.

- La ARN solicitará la autorización a los Titulares de los datos personales y mantendrá las pruebas de ésta, cuando en virtud de las funciones de promoción, divulgación y capacitación, realice invitaciones a charlas, conferencias o eventos que impliquen el Tratamiento de Datos Personales con una finalidad diferente para la cual fueron recolectados inicialmente.

- Las principales finalidades para el tratamiento de datos personales que corresponden a la ARN en ejercicio de sus funciones legales se relacionan con:
  - Brindar información sobre los servicios que ofrece la ARN.
  - Invitar a eventos y capacitaciones, cursos o seminarios organizados por la ARN.
  - Perfilar nuestros usuarios y evaluar los servicios de la ARN.
  - Adelantar los trámites y servicios que tiene a cargo la ARN, en ejercicio de sus funciones.
  - Realizar encuestas relacionadas con la misión de la ARN.

7.1. LINEAMIENTOS ESPECÍFICOS PARA EL TRATAMIENTO DE DATOS PERSONALES EN LA ARN:

- La ARN mantendrá los datos personales bajo las siguientes características: ser confiable, veraz y completo, siempre y cuando el Titular informe oportunamente sus novedades y sea veraz la información suministrada a la entidad.
- Los Datos Personales solo serán Tratados por aquellos colaboradores de la ARN que cuenten con el permiso para ello, o quienes dentro de sus funciones tengan a cargo la realización de tales actividades o por los Encargados.
- La ARN como responsable del tratamiento de los datos personales contenidos en sus bases de datos contará con el apoyo del Comité Institucional de Gestión y Desempeño o quien haga sus veces, en la orientación de las políticas, y hacer su seguimiento.
- La Mesa de Seguridad apoyará al Comité Institucional de Gestión y Desempeño o quien haga sus veces en la emisión de recomendaciones, realizar seguimiento los planes establecidos y a novedades relacionadas con protección de datos personales.

- La Oficina Asesora de Planeación tendrá el rol de Gestor en la ARN llevando el control de registro de las bases de datos (automatizadas y manuales) con información personal que hay en la entidad y apoyará el ingreso de la información en el Registro Nacional de Base de Datos de la Superintendencia de Industria y Comercio.
- Cada una de las bases de datos personales registradas por el Gestor contarán con un administrador de base de datos personales, quien tendrá a cargo el tratamiento de los datos personales.
- La ARN facilitará el derecho constitucional a conocer, actualizar y rectificar la información recogida en bases de datos y los demás derechos, libertades y garantías a las que se refieren los artículos 15 y 20 de la Constitución Política sobre derecho a la intimidad y derecho a la información, respectivamente.
- Las siguientes disposiciones aplican a los datos personales registrados en cualquier base de datos que gestiona la ARN en sus procesos. Entiéndase como base de datos automatizadas y base de datos manuales o archivos.

  - Todo Dato Personal que no sea Dato Público se tratará por la ARN como confidencial, aun cuando la relación contractual o el vínculo entre el Titular del Dato Personal y la ARN haya finalizado. A la terminación de dicho vínculo, tales Datos Personales deben continuar siendo tratados de acuerdo con lo dispuesto en el presente manual y los procedimientos que establezca la Secretaría General sobre Gestión Documental.
  - Cada dependencia de la ARN debe anonimizar los actos administrativos y/o documentos de carácter público que contengan datos personales, para su publicación.
  - El valor de la anonimización prevalece en entornos y estrategias de inteligencia de negocio (BI), datos abiertos (Open data) o datos masivos (big data), que apoyen a la entidad y la ciudadanía. Para ello, se tendrá en cuenta un análisis de riesgos y consideración para que este proceso no implique la pérdida de gran cantidad de información y datos que hagan ineficaces la información publicada.
  - El Titular, directamente o a través de las personas debidamente autorizadas, podrá consultar sus Datos Personales en todo momento y especialmente cada vez que existan modificaciones en las Políticas de Tratamiento de la información.
  - La ARN suministrará, actualizará, ratificará o suprimirá los Datos Personales a solicitud del Titular para corregir información parcial, inexacta, incompleta, fraccionada que induzca al error o aquella que haya sido tratada previa a la vigencia de la ley y/o aplicación de esta política que no tenga autorización o sea prohibida.

- Todos los colaboradores de la ARN son responsables de dar cumplimiento a la normatividad y lineamientos de protección de datos y deberán reportar cualquier violación a las mismas a su jefe inmediato.
- La ARN es rigurosa en la aplicación de las políticas de tratamiento de la información cuando se trate del uso de datos personales de los niños, niñas y adolescentes asegurando la protección de sus derechos.
- La ARN podrá intercambiar información de Datos Personales con entidades del Estado, de impuestos, organismos de investigación y autoridades judiciales, cuando la soliciten en ejercicio de sus funciones.
- Los Datos Personales sujetos a tratamiento deberán ser manejados proveyendo para ello todas las medidas tanto humanas como técnicas para su protección, brindando la seguridad de que ésta no pueda ser copiada, adulterada, eliminada, consultada o de alguna manera utilizada sin autorización o para uso fraudulento.
- Cuando finalice alguna de las labores de tratamiento de Datos Personales por los colaboradores o Encargados del tratamiento, y aun después de finalizado su vínculo o relación contractual con la ARN, éstos están obligados a mantener la reserva de la información de acuerdo con la normatividad vigente en la materia.
- La ARN divulgará a sus colaboradores, contratistas y terceros encargados del tratamiento las obligaciones que tienen en relación con el tratamiento de Datos Personales mediante campañas y actividades de sensibilización y trasferencia de conocimiento.
- El titular podrá entrar en contacto con la ARN sobre información relacionada con la protección de datos personales a través de su página web: www.reintegracion.gov.co, telefónicamente comunicándose al teléfono fijo al (+57-1)01 8000 911 516, desde un celular Claro o Movistar #516 (atención de lunes a viernes de 8:00 a.m. a 6:00 p.m. y sábados de 8:00 a.m. a 1:00 p.m.).

  También puede acceder al chat de atención a la ciudadanía o ingresar al Sistema de registro de Peticiones, Quejas, Reclamos, Sugerencias o Denuncias (PQRS-D) de la página web, las cuales serán atendidas de acuerdo a los protocolos establecidos en el Manual del Sistema de PQRS-D (AC-M-01).
- Los directores, subdirectores, Jefes de Oficina, Coordinadores y colaboradores deben reportar las bases de datos con información personal que administren e informarán las novedades de su administración al Gestor, así como las nuevas bases de datos que se constituyan.
- La ARN implementará procedimientos para garantizar el cumplimiento de sus políticas de tratamiento de la información personal.

- El incumplimiento de las políticas de tratamiento de la información acarreará las sanciones contempladas en el Código único Disciplinario y normas concordantes.
- La ARN dará cumplimiento a las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio en materia de Protección de datos personales.
- Las políticas establecidas por la ARN respecto al tratamiento de Datos Personales podrán ser modificadas en cualquier momento. Toda modificación se realizará con apego a la normatividad legal vigente, y las mismas entrarán en vigencia y tendrán efectos desde su publicación a través de los mecanismos dispuestos por la ARN para que los titulares conozcan la política de tratamiento de la información y los cambios que se produzcan en ella.

7.2. LINEAMIENTOS PARA LOS ENCARGADOS DEL TRATAMIENTO DE DATOS PERSONALES:

- La ARN suministrará a los Encargados del Tratamiento de Datos Personales según el caso, información de datos personales únicamente cuando lo requiera en virtud de sus funciones legales y, cuando excepcionalmente éstas no apliquen, con la autorización del Titular
- La ARN deberá garantizar que la información que le suministra a los Encargados del Tratamiento de Datos Personales sea veraz, completa, exacta, actualizada, comprobable y comprensible. Adicionalmente le comunicará de manera oportuna todas las novedades a que haya lugar para que la información siempre se mantenga actualizada.
- La ARN informará al Encargado del Tratamiento de Datos Personales, cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.
- La ARN debe exigir al Encargado del Tratamiento de Datos Personales que, en todo momento, se respeten las condiciones de seguridad y confidencialidad de la información del Titular establecidas por la SIC.

7.3. RESPONSABILIDADES DE LOS ADMINISTRADORES DE BASES DE DATOS PERSONALES:

- Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- Solicitar y conservar, en las condiciones previstas en la citada ley, copia de la respectiva autorización otorgada por el Titular.

- Informar debidamente el Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
- Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a éste se mantenga actualizada.
- Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.
- Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la normatividad legal vigente.
- Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.
- Tramitar las consultas y reclamos formulados en los términos señalados en la normatividad legal vigente
- Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.
- Informar a solicitud del Titular sobre el uso dado a sus datos.
- Informar al jefe inmediato cuando se presenten violaciones a las normas y procedimientos establecidos para protección de datos.
- Atender las instrucciones y requerimientos que imparta el Comité Institucional de Gestión y Desempeño o quien haga sus veces y la Superintendencia de Industria y Comercio” en la relacionado con la protección de datos personales.

VIII. CONTROLES DE LA DOCUMENTACIÓN DEL SGSI

El Manual del Sistema de Gestión de Seguridad de la Información está articulado con los demás documentos complementarios que se han documentado y todos los colaboradores pueden acceder a dichos documentos para consulta a través del SIGER.

IX. REVISIÓN

El Manual del Sistema de Seguridad de la Información será revisado anualmente o antes si existen modificaciones que así lo requieran, para garantizar que sigue

siendo oportuno, suficiente y eficaz. Esta revisión será liderada por el responsable de Seguridad y la Mesa de Seguridad.

X. ACCIONES POR INCUMPLIMIENTO DE LAS POLÍTICAS DEL SGSI

Para los colaboradores que hayan cometido alguna violación de la Política de Seguridad de la Información se establecerá un procedimiento que atenderá Control Interno Disciplinario, quien recomendará a la Secretaría General las acciones a seguir según sea el caso.

XI. DOCUMENTOS DE REFERENCIA Y FUENTES DE INFORMACIÓN

- Decreto 1008 de 2018. Política de Gobierno Digital
- Manual de Gobierno Digital
- Estándar ISO 27001 Versión 2013
- Ley 1581 de 2012 - Ley de protección de datos personales
- Ley 1712 de 2014 – Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- Políticas de tratamiento de la información personal en la Superintendencia de Industria y Comercio, www.sic.gov.co
- CONPES 3854 de 2016 - Política Nacional De Seguridad Digital
- Manual de Seguridad de la Información de la Presidencia de la República.

Política Nacional de Gestión Integral de Residuos de Aparatos Eléctricos y Electrónicos