AGENCIA PARA LA REINCORPORACIÓN Y NORMALIZACIÓN (ARN)

MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C. OCTUBRE DE 2020

TABLA DE CONTENIDO

1. 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, acorde con la normatividad vigente.

2. 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.

3. ALCANCE

El presente manual aplica a todos los procesos de la Agencia para la Reincorporación y la Normalización- ARN y las directrices aquí definidas deben ser aplicadas por todos los empleados públicos, contratistas. y terceros que presten sus servicios o tengan algún tipo de relación con la ARN, para el adecuado cumplimiento de sus funciones y obligaciones y para conseguir un adecuado nivel de protección de las características de calidad y seguridad de la información, contribuyendo con su participación en la toma de medidas preventivas y correctivas para el logro del objetivo y la finalidad del presente manual.

4. DEFINICIONES

ACTIVO: Según [ISO/IEC 13335-1:2004] 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, el cual posee un valor y es necesario para realizar los procesos misionales y operativos de la ARN. Se pueden clasificar de la siguiente manera: datos, hardware, software (tales como: aplicaciones, herramientas, sistemas de información, portales y servicios.

ACTIVO CRÍTICO: Instalaciones, sistemas y equipos los cuales, si son destruidos, o es degradado su funcionamiento o por cualquier otro motivo no se encuentran disponibles, afectaran el cumplimiento de los objetivos estratégicos de la ARN.

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

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. Ejemplo: Procesador de texto, herramienta para apoyo a la gestión, software para intercambio de información con otra entidad. Por ejemplo: SIGOB, SIGER.

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.

AUTOR: Persona física que realiza la creación intelectual.

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 empleados públicos.

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

BYOD (Bring Your Own Device): dispositivos electrónicos personales tales como teléfonos inteligentes, tabletas, computador portátil, computador de escritorio.

CIBERACTIVO: Se identifica como foco de la ciberseguridad los activos digitales como datos, dispositivos y sistemas que permiten a la organización cumplir con sus objetivos de negocio.

CIBERACTIVO CRÍTICO: que es crítico para la operación de un activo crítico y es calificado como aquel que tiene al menos una de las siguientes características:

- El ciberactivo usa un protocolo enrutable para comunicarse afuera del perímetro de seguridad electrónica, o,
- El ciberactivo usa un protocolo enrutable con un centro de control, o,
- El ciberactivo es accesible por marcación.

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)

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”.

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

DERECHOS DE AUTOR: Es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

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: Propiedad o característica de los activos consistente en que los usuarios o procesos autorizados tiene acceso a los mismos cuando lo requieren.

EVENTO: Incidente o situación, que ocurre en un lugar determinado durante un periodo de tiempo determinado. Este puede ser cierto o incierto y su ocurrencia puede ser única o ser parte de una serie.

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad afectando la disponibilidad, integridad o confidencialidad de uno o más activos de información.

GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL: Conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar y controlar 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).

HARDWARE: Son todos los equipos utilizados para gestionar la información y las comunicaciones. Ejemplo: servidores, switches, equipo de cómputo, impresoras, escáner.

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.

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.

INFORMACIÓN PÚBLICA 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.

INFORMACIÓN PÚBLICA: Es aquella información que puede ser distribuida abiertamente al público sin que cause daño alguno a la entidad, a sus contratistas, otras dependencias o a otras entidades.

INFORMACIÓN PÚBLICA 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.

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.

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN. Un incidente de seguridad de la información está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

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, 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 empleado público 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.

ONE DRIVE: Es la plataforma en la nube de Microsoft que permite guardar archivos o documentos en línea y acceder a ellos desde cualquier lugar o equipo con conexión a Internet. Sitio para almacenamiento virtual en la nube de la información pública de la Entidad.

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.

PORTALES: (En Internet), conjunto de páginas reunidas bajo una marca, dirección, tema, asunto o interés. Por ejemplo: Portal Web de la ARN. – personal que labora en la entidad: Son todos los empleados públicos, contratistas 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.

PROPIEDAD INTELECTUAL: Es una disciplina normativa que protege las creaciones intelectuales provenientes de un esfuerzo, trabajo o destreza humanos, dignos de reconocimiento jurídico. La Propiedad Intelectual comprende:

- El derecho de autor y los derechos conexos;

- La propiedad industrial (que comprende la protección de los signos distintivos, de las nuevas creaciones, los circuitos integrados, los secretos industriales);
- Las nuevas variedades vegetales.

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.

RANSOMWARE: Tipo de malware que toma por completo el control del equipo bloqueando o cifrando la información del usuario para, a continuación, pedir dinero a cambio de liberar o descifrar los archivos del dispositivo.

REGISTRO NACIONAL DE DERECHO DE AUTOR: Es un servicio que presta el Estado a través de la Unidad Administrativa Especial Dirección Nacional de Derecho de Autor, para todo el territorio nacional. Su finalidad es brindarles a los titulares de derecho de autor y derechos conexos un medio de prueba y de publicidad a sus derechos, así como a los actos y contratos que transfieran o cambien ese dominio amparado por la ley. Igualmente, ofrece garantía de autenticidad y seguridad a los títulos de derecho de autor y de derechos conexos y a los actos y documentos que a ellos se refiere.

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.

SERVICIOS: Utilidad inmaterial o intangible provista para atender una necesidad. Se refiere a los servicios internos que se suministran internamente entre las dependencias de una organización; los externos son aquellos que la organización suministra a clientes y usuarios externos.

SEGURIDAD DIGITAL: es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país

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.

SISTEMAS DE INFORMACIÓN: conjunto de recursos que sirven como soporte para el proceso de captación, transformación y comunicación de información. Son considerados fuente única de datos útiles para apoyar o argumentar las decisiones institucionales que incluyen estrategia, procesos, organización, recursos (humanos, tecnológicos, financieros), información confiable, entre otros. Por ejemplo: Sistema de Información para la reintegración – SIR.

SISTEMAS DE VIDEOVIGILANCIA (SV): consiste en un conjunto de cámaras de seguridad implementadas con la finalidad de garantizar la seguridad de bienes o personas en un lugar determinado son considerados como un medio idóneo para realizar el monitoreo y la observación de actividades en escenarios laborales y públicos.

SOFTWARE: Conjunto de herramientas intangibles que permiten a un computador realizar una tarea, son todas las herramientas, aplicativos, sistemas de información o portales que se utilizan para la gestión de la ARN.

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: (Suplantación de identidad), en términos de seguridad de redes, hace referencia al uso de técnicas a través de las cuales un atacante, generalmente con usos maliciosos o de investigación, se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación.

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.

TERCERA PARTE. Persona u organismo reconocido por ser independiente con relación al asunto en cuestión de las partes involucradas.

TRATAMIENTO DE DATOS PERSONALES: cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión". En el caso de las imágenes de personas determinadas o determinables, operaciones como la captación, grabación,

transmisión, almacenamiento, conservación, o reproducción en tiempo real o posterior, entre otras, son consideradas como Tratamiento de datos personales y, en consecuencia, se encuentran sujetas al Régimen General de Protección de Datos Personales.

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 al empleado público y contratista, 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.

VIRTUAL PROTOCOL NETWORK (VPN): Es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

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.

WEB SERVICES: Es una tecnología que utiliza un conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones.

5. MARCO NORMATIVO

El Manual del Sistema de Gestión de Seguridad de la Información de la ARN se encuentra alineado con el marco normativo definido para las Entidades Públicas y para el Sector Presidencia al cual pertenece la ARN. A continuación, se hace referencia a la normatividad básica a partir de la cual tienen sustento el desarrollo e implementación de la tecnología y los sistemas de información de la ARN:

- Decreto 4138 de 3 de noviembre de 2011 - Por el cual se crea la Agencia Colombiana para la Reintegración.
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales
- Ley 1712 del 6 de marzo de 2014 - Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.
- Documento CONPES No. 3854 del 11 de abril de 2016 - Política Nacional de Seguridad Digital.
- Decreto Ley No. 897 del 29 de mayo de 2017 - Por el cual se modifica la estructura de la Agencia Colombiana para la Reintegración de Personas y Grupos Alzados en Armas y se dictan otras disposiciones.
- Decreto 1008 del 14 de junio de 2018 - Gobierno Digital.
- Decreto 1212 del 13 de julio de 2018 - Por medio del cual se adiciona una función a la Agencia para la Reincorporación y la Normalización y se modifica el Decreto 4138 de 2011.
- Decreto 620 de 2020 Lineamientos para la implementación de los Servicios Ciudadanos Digitales.

En el Sistema Integrado de Gestión se encuentra dispuesto el Normograma del proceso de gestión de tecnologías de la información.

6. CONSIDERACIONES GENERALES

6.1 ASPECTOS TRANSVERSALES INSTITUCIONALES

El presente manual indica los lineamientos y directrices que emite la Dirección General en asuntos tales como: Seguridad de la información, Protección de datos personales y Derechos de autor, para precisar acerca de procedimientos o acciones de las dependencias responsables se requiere consultar la documentación de cada proceso disponible en SIGER, entre otros los siguientes manuales: DE- M-02 Manual de gestión del riesgo, DE-M-04 Manual del SIGER, DE-M-05 Manual para la gestión de proyectos, TH-M-01 Manual de teletrabajo, lineamientos de trabajo en casa, AC-M-01 Manual del sistema de PQRS-D, GA-M-01 Manual de seguridad preventiva, GA-M-02 Manual para el manejo y control administrativo de los bienes de propiedad de la Entidad,CO-M-01 Manual de operación proceso de gestión de comunicaciones, GD-M-02 Manual producción de documentos, DE-M-06 Manual de Protección de Datos, BS-M-01 Manual de contratación, supervisión e interventoría.

6.2 CONTROLES DE LA DOCUMENTACIÓN DEL SGSI

El Manual del Sistema de Gestión de Seguridad de la Información está articulado con los demás documentos complementarios relacionados y todos los empleados públicos y contratistas pueden acceder a dichos documentos para consulta a través del SIGER.

6.3 REVISIÓN

El Manual del Sistema de Seguridad de la Información es revisado anualmente o antes si existen modificaciones que así lo requieran, para garantizar que sigue siendo oportuno, suficiente y eficaz. Esta revisión es liderada por el responsable de Seguridad y la Mesa de Seguridad.

6.4 ACCIONES POR INCUMPLIMIENTO DE LAS POLÍTICAS DEL SGSI

Para los empleados públicos y contratistas que hayan cometido alguna violación de la Política de Seguridad de la Información se establece un procedimiento que atiende Control Interno Disciplinario, quien recomienda a la Secretaría General las acciones a seguir según sea el caso.

7 CONTENIDO Y DESARROLLO

I. DE LA SEGURIDAD DE LA INFORMACIÓN

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

El Sistema de Gestión de Seguridad de la Información-SGSI es aplicable a todos procesos, plataformas tecnológicas y los activos de información identificados en la ARN el cual debe ser adoptado por la alta dirección, empleados públicos, contratistas y terceros en razón al cumplimiento de la misionalidad de la entidad y a sus funciones u obligaciones contractuales que incluyen aspectos relacionado con compartir, utilizar, recolectar, procesar, intercambiar o consultar información. Así mismo, el SGSI aplica a toda la información creada, procesada o utilizada por la ARN, sin importar el medio, formato o presentación o lugar en el cual se encuentre.

El SGSI está incorporado dentro del Sistema Integrado de Gestión y es responsable de su adopción el Director General de la ARN.

2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La Dirección General de la ARN declara el compromiso con esta política de Seguridad de la Información y la protección de datos para todos los procesos, plataformas tecnológicas y activos de información involucrados en su alcance.

2.1 COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO

El Comité Institucional de Gestión y Desempeño como un órgano rector, articulador y ejecutor, de las acciones y estrategias a nivel institucional, interviene para la adecuada dirección, implementación, implantación, gestión y mantenimiento del SGSI y de la Política de Gobierno Digital en la ARN. 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 empleados públicos y contratistas, 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 está conformada por:

- El Asesor de Estrategia y 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 jefe de la Oficina de Tecnologías de la Información
- 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 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 empleados 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 empleados públicos 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 designe el Director General, 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, así como, la seguridad digital.
- 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.
- Verificar la Gestión de Activos de Información que está a cargo de la Oficina Asesora de Planeación.
- Apoyar a la Oficina de Control Interno de Gestión en el cumplimiento de la Gestión de riesgos de seguridad de la información y seguridad digital.
- Definir y generar métricas de seguridad de la información, en el marco del SGSI.
- Supervisar la respuesta a incidentes, así como, la investigación de las violaciones de la seguridad, ayudando con las investigaciones disciplinarias y legales necesarias.

- ***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 brinda 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 la ocurrencia de 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 y al responsable de Seguridad de la Información los cambios necesarios.
- Preparar y monitorear el programa de sensibilización en seguridad informática para todo los empleados públicos y contratistas.
- Probar la arquitectura de seguridad para evaluar la fortaleza de la seguridad y para detectar y actuar ante 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 informática.
- Realizar las recomendaciones, monitorear y verificar su aplicación.

2.3 ROLES Y RESPONSABILIDADES EN 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 de 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 todo los empleados públicos y contratistas de la Entidad.

- ***Personal Directivo de la Agencia para la Reincorporación y la Normalización***

El Señor Director General, el Secretario General, el Director Programático de Reintegración, el Jefe Oficina Asesora de Planeación, el Jefe Oficina Asesora Jurídica, el Jefe Oficina Asesora de Comunicaciones, el Jefe Oficina de Tecnologías de la Información y los 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 empleados públicos y contratistas a su cargo, para que toda la entidad esté alineada con el cumplimiento de los objetivos del SGSI.

- ***Empleados públicos y contratistas de la Agencia para la Reincorporación y la Normalización***

Los empleados públicos y contratistas de la ARN, 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.

Todo los empleados públicos y contratistas 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 empleados públicos deben firmar el documento “Acta de compromiso y autorización sobre confidencialidad y manejo de la información”.

- ***Propietario de los activos de información***

Es el empleado público o contratista 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 empleado público o contratista 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 empleado público o contratista 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 deben 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 que 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 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 y la normatividad aplicable.
- Conocer las responsabilidades y asumir las 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, no exponerlas, ni entregarlas a otras personas, ya que son de carácter personal y con uso exclusivo.
- Si los empleados públicos o contratistas tienen sospechas de que su acceso autorizado ha sido vulnerado o está siendo utilizado por otra persona, debe iniciar el cambio de contraseña y comunicar éste u otros incidentes de seguridad de la información a la Mesa de Servicios a la extensión 10999 o al correo soporte@reincorporacion.gov.co.

- ***Personal con acceso privilegiado***

Los empleados públicos y contratistas 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 empleado público o contratista.

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***:

Corresponde a un empleado público o responsable designado perteneciente a la dependencia usuaria, responsable del manejo funcional del cada sistema de información y/o aplicación, dichas actividades deben estar alineadas a los procesos definidos para cada área. La delegación es responsabilidad del jefe del área.

Las responsabilidades específicas líder o administrador funcional son:

- Conocer los elementos que soportan el funcionamiento del sistema de información, aplicación o infraestructura de TI, con el fin de asegurar que los requerimientos funcionales definidos para su desarrollo y que estén acordes a los procesos de la Entidad.
- Liderar el análisis desde el punto de vista funcional del del sistema de información, aplicación o infraestructura de TI que lidera y establecer las necesidades y requerimientos.
- Administrar los usuarios del del sistema de información, aplicación o infraestructura de TI, actividad que incluye actualización e inactivación de usuarios y su asociación a cada uno de los roles.
- Validar y Aprobar la funcionalidad del sistema de información, aplicación o infraestructura de TI desarrollada y/o actualizada con el fin de garantizar que cumpla con los requerimientos del proceso.
- Capacitar y socializar a los usuarios de del sistema de información, aplicación o infraestructura de TI bajo su responsabilidad tanto en el proceso como en la utilización del mismo.
- Responder los requerimientos de mesa de servicios y soporte funcional sobre del sistema de información, aplicación o infraestructura de TI bajo su responsabilidad.
- Participar en la elaboración, divulgación del plan de contingencia que debe ejecutarse cuando el sistema de información, aplicación o infraestructura de TI no se encuentre disponibles para garantizar la continuidad en el proceso funcional.

- Informar a la mesa de servicios los incidentes que detecte en la información del del sistema de información, aplicación bajo su responsabilidad con el fin de que se realicen las acciones necesarias.
- Atender desde el punto de vista funcional los procesos de auditoría de del sistema de información, aplicación o infraestructura de TI cuando sea requerido, implementando acciones necesarias para la mejora.

- ***Líder técnico****:*

Corresponde a un empleado público o responsable designado de la Oficina de Tecnologías de la Información, que tiene el conocimiento técnico necesario para atender los requerimientos realizados por un área funcional para un determinado sistema de información o aplicación. La delegación es responsabilidad del jefe de la Oficina de Tecnologías de la Información.

Las responsabilidades específicas líder técnico son:

- Liderar el proceso de especificación de requerimientos desde el punto de vista técnico, garantizando que se incluyan las necesidades expresadas por el líder funcional y que se genere la documentación requerida para este proceso.
- Liderar cada una de las etapas de desarrollo de sistemas de información, aplicaciones, portales o servicios de TI garantizando el cumplimiento de los requerimientos funcionales y técnicos planteados en el proyecto.
- Propender la generación, revisión y aprobación de la documentación técnica requerida para el desarrollo y/o mantenimiento de los sistemas de información /aplicaciones y servicios de TI.
- Validar que se cumpla con toda la documentación requerida para la entrega a producción de los sistemas de información/aplicaciones y servicios de TI.
- Prestar el soporte técnico a los sistemas de información/aplicaciones y servicios de TI bajo su responsabilidad de manera eficaz y oportuna.
- Realizar las actualizaciones necesarias en la documentación técnica de los sistemas de información, aplicaciones y servicios de TI bajo su responsabilidad.
- Definir los niveles de disponibilidad y capacidad que se requieren para los sistemas de información, aplicaciones y servicios de TI bajo su responsabilidad.
- Apoyar en la elaboración, divulgación del plan de contingencia y pruebas que debe ejecutarse cuando el sistema de información, aplicación o infraestructura de TI no se encuentre disponibles para garantizar la continuidad en el proceso funcional.
- Capacitar líder funcional en la operación y manejo de los sistemas de Información/aplicaciones y servicios de TI bajo su responsabilidad.

- ***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 empleado público 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 requerimientos e incidentes de hardware y software y en relación con sus funciones tienen 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 está 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 elaboran el Plan de Preservación Digital
- La Oficina de Tecnologías de la Información está encargada de la seguridad informática de la ARN.

3 POLÍTICAS

3.1 POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

La Agencia para la Reincorporación y la Normalización, mediante la adopción e implementación del Modelo de Seguridad y Privacidad de la Información-MSPI articulado con el Sistema de Gestión de Seguridad de la información-SGSI, está comprometida con la preservación de la confidencialidad, integridad, disponibilidad, legalidad y no repudio de toda información relacionada con su

misionalidad mediante una gestión integral de riesgos, la implementación de controles y mecanismos para la prevención de incidentes para dar cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua y desempeño del Sistema de Gestión de Seguridad de la Información, enfocado en liderar y coordinar el diseño e implementación de la política pública de reintegración y reincorporación, contribuyendo a la convivencia, la cultura de la legalidad, la reconciliación y el desarrollo sostenible.

3.2 OBJETIVOS DE SGSI

- Gestionar los riesgos de seguridad digital, para que sean conocidos y según su impacto sean atendidos de una forma documentada, eficiente y adaptada al entorno y la tecnología.
- Proteger la información de la gestión de la Agencia para la Reincorporación y la Normalización y la tecnología utilizada para su procesamiento, asegurando el cumplimiento de los principios de confidencialidad, integridad y disponibilidad de la información.
- Propender por la continuidad de los servicios de gestión de la Entidad y tecnología de la información frente a incidentes.
- Construir una cultura organizacional en seguridad digital al interior de la entidad con el fin de adoptar las buenas prácticas y comportamientos seguros en el manejo de información.

3.3 CIBERDEFENSA Y CIBERSEGURIDAD EN LA ARN

En la ARN se da 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, es 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, ransomware, 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 cuentan 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, los procesos de contratación que se adelanten en la ARN deben seguir las disposiciones descritas en el documento BS-M-01 Manual de contratación, supervisión e interventoría.

De acuerdo con lo anterior, las adquisiciones de tecnologías de la información (hardware, software, servicios, aplicativos), que se adelanten en la entidad cumplen 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 el caso de proyectos de tecnologías de la información se designa un líder que es el responsable de detectar las necesidades de los usuarios y gestionar los recursos

para obtener los resultados esperados en los plazos previstos y con la calidad necesaria.

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 de la Dependencia o quien este delegue con su correspondiente justificación para su respectivo análisis de viabilidad.

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

Consiste en aplicar buenas prácticas en la gestión de los sistemas de información, aplicativos o servicios de tecnologías de la información que se encuentran en producción con el fin de atender las necesidades de la entidad y de los usuarios.

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.
- Actualizar el inventario de todos los sistemas de información, aplicativos y servicios.
- Para el acceso a los sistemas de información, aplicativos o servicios, los grupos de Talento Humano y el de Gestión Contractual informan las novedades de ingreso, traslado, retiro, vacaciones, incapacidades, suspensiones, del empleado público o contratista, para configurar los roles y privilegios de los usuarios.

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 los controles a los empleados públicos y contratistas 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 proporciona a los empleados públicos y contratistas los equipos informáticos y los programas instalados en ellos.
- Los empleados públicos y contratistas deben utilizar únicamente los programas y equipos autorizados por la Oficina de Tecnologías de la Información.

- Para los terceros se deben 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 empleados públicos y contratistas, 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 empleados públicos y contratistas 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 empleados públicos y contratistas deben 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 deben 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.
- Todo los empleados públicos y contratistas propenden 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.
- Todo los empleados públicos y contratistas propenden 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 y será reportado al Oficial de seguridad de la información para que se tomen las medidas correspondientes.
En caso de ser necesario y previa autorización de la Mesa de Seguridad de la ARN, el personal de la Oficina de Tecnologías de la Información de la ARN podrá 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 información de la ARN deben ser identificados, clasificados y controlados para garantizar el uso adecuado, protección y la recuperación ante desastres de acuerdo con lo establecido en el documento DE-I-03 Instructivo para la actualización de la matriz de activos de información.

El Grupo de Almacén e Inventarios, debe llevar y administrar el inventario valorizado de hardware y software 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 pueden 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 o medios extraíbles 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 realiza la actualización del inventario de sus activos de información mínimo una vez al año, bajo la responsabilidad de cada propietario y liderado por la Oficina Asesora de Planeación.

La ARN es propietaria de los activos de información y los administradores de estos activos son los empleados públicos y contratistas 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 clasifica 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 los empleados públicos y contratistas y 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 empleados públicos y contratistas 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

Todo los empleados públicos y contratistas 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 empleados públicos y contratistas, 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 los empleados públicos y contratistas, 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 comunicaciones unificadas (Teams) y Correo Electrónico**

Dichas herramientas son para apoyo a las funciones y responsabilidades de los empleados públicos y contratistas 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 de correo institucional que administra la Oficina Asesora de comunicaciones.
- Todo mensaje SPAM o CADENA debe ser inmediatamente reportado al correo soporte@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 soporte@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 son 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.
- Está expresamente prohibido crear, almacenar o intercambiar mensajes que violen las leyes de material protegido por la ley de derechos de autor, normas sobre seguridad de la información y protección de datos personales.
- Está expresamente prohibido Crear, enviar, alterar, borrar mensajes suplantando la identidad de un usuario.
- 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.

La información transmitida es de carácter confidencial, está amparada por la Ley 1581 de 2012 y demás reglamentación relacionada con habeas data, junto con todas las disposiciones de seguridad de la información y protección de datos personales. La información intercambiada es de uso exclusivo de la ARN y no puede ser divulgada a ninguna parte externa…".

- 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.
- Antes de enviar un correo el usuario deberá verificar que esté dirigido solamente a los interesados y/o a quienes deban conocer o decidir sobre el tema, evitando duplicidades o desmejoramiento en el servicio y operación de la red.
- El mantenimiento del buzón de correo será responsabilidad del usuario y se deberá conservar únicamente los mensajes necesarios con el fin de no exceder el máximo límite de almacenamiento.
- El soporte técnico sobre la configuración de aplicaciones y correo electrónico es brindado por la Oficina de Tecnologías de la Información únicamente para los equipos de cómputo propiedad de la entidad.
- Como lo establece la ley 1273 de 2009, de delitos informáticos, está prohibida la Interceptación de datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte, por lo que está prohibida la interceptación de los mensajes de correo electrónico sin autorización legal.
- Asimismo, está prohibido el acceso abusivo a un sistema informático, por lo tanto, está prohibido acceder al buzón de correo electrónico de otros funcionarios sin la debida autorización.

- **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 empleados públicos y contratistas; 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 empleado público y contratista 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 el personal 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 empleado público y contratista 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, es el personal 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 empleado público y/o contratista 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 Siendo software libre para su uso institucional sea expresamente autorizado por la Oficina de Tecnologías de la Información.
- Los únicos autorizados para instalar y/o desinstalar programas o herramientas de software es el personal 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 debe 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 es almacenada en las bases de datos de los sistemas de información dispuestos para este fin, para garantizar su seguridad y respaldo.
- La información CONFIDENCIAL debe 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.
- La ARN suministra una cuota de almacenamiento de la información en un servidor de archivos con los permisos necesarios para que cada usuario guarde la información que crea importante y sobre ella se garantizará la disponibilidad en caso de un daño en el equipo asignado, esta información será guardada durante el periodo establecido.
- El acceso a la información RESERVADA y/o CONFIDENCIAL es autorizado por el propietario de la información.
- Los usuarios solo tendrán acceso a los datos y recursos autorizados, y serán responsables disciplinaria y legalmente de la divulgación no autorizada de esta información.
- Los acuerdos de No-Divulgación de Información que se suscriban con terceros deben 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.
- El Grupo de Talento Humano se encargará de tramitar la firma de Acuerdo de Tratamiento de Datos Personales de los empleados públicos y el Grupo de Gestión Contractual de los contratistas de la ARN y guardar las evidencias correspondientes.
- El Grupo de Gestión Contractual se encarga 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 encarga 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 debe reposar copia en la carpeta contractual.

3.9 POLÍTICA DE GESTIÓN DE ALMACENAMIENTO

Con el objetivo de mantener protegida y realizar una administración adecuada de la información de la ARN que se encuentre en las unidades de almacenamiento y propender que se cumplan los principios de seguridad de la información relacionados con la confidencialidad, integridad y disponibilidad, la Oficina de Tecnologías de la Información pone a disposición de las diferentes dependencias tres (3) recursos de almacenamiento los cuales son: carpetas compartidas, carpetas de trabajo y OneDrive.

El manejo de la información debe realizarse de acuerdo con lo establecido en este documento en el numeral *3.8 Política del uso aceptable de los activos Regla No 4: del manejo de la información*.

3.9.1 De las carpetas compartidas y de trabajo

Las carpetas compartidas sobre la infraestructura ofrecida por OTI serán administradas por las diferentes dependencias quienes deben dar un buen uso la información y de la cuota y permisos en estas carpetas.

La Oficina de Tecnologías de la Información, asigna los permisos y accesos sobre las carpetas compartidas, en atención a la disposición que realice el responsable de las carpetas usando los siguientes criterios:

• Permisos de Lectura
• Permisos de Lectura y Escritura

Dichas solicitudes deben ser tramitadas a través de la Mesa de Servicios por el Jefe de Dependencia o Coordinador, anexando el formato TI-F-01 Solicitud de Usuario y/o Recursos Tecnológicos establecido.

El administrador de cada carpeta deberá fijar el límite de tiempo durante el cual estará publicada la información y compartido el recurso en la infraestructura ofrecida por la OTI.

Cada administrador de las carpetas compartidas deberá realizar mínimo de manera semestral una depuración de la información con el fin de optimizar los recursos de almacenamiento disponible.

Cuando el empleado público o contratista desarrolle labores fuera de las sedes de la entidad, si requiere acceso a las carpetas compartidas debe realizar la conexión a través de la VPN que dispone la OTI para tener acceso a este recurso; en caso de utilizar un equipo de cómputo personal debe contar con un antivirus actualizado para la conexión.

Los recursos de almacenamiento como carpetas compartidas y OneDrive, aprovisionados por la ARN para los usuarios, deben estar exentos de publicaciones de archivos de tipo ejecutable como .exe, .bat, .dll, entre otros), si la dependencia requiere hacer uso de alguna de las extensiones mencionadas, debe informar de la necesidad a la a la OTI para realizar las respectivas recomendaciones y el acompañamiento en el uso, incluyendo el ajuste de las políticas de seguridad informática dado caso se requiera.

La OTI realiza monitoreo e informes periódicos a los administradores y responsables de las carpetas compartidas y OneDrive, en relación con el nivel de utilización del espacio dispuesto, usuarios con acceso a los recursos, entre otras variables, con el fin de realizar una validación por parte de los responsables de cada dependencia para la correcta administración de los recursos de almacenamiento.

Los recursos de almacenamiento provistos por la ARN para los usuarios deben ser utilizados para alojar archivos derivados de las actividades laborales u obligaciones contractuales.

Se requiere abstenerse de alojar archivos personales, música, videos, imágenes y cualquier otro tipo de archivo no relacionado con el cumplimiento de las actividades de los empleados públicos o contratistas.

Los nombres a los archivos y carpetas deben tener en cuenta las disposiciones definidas por el Grupo de Gestión Documental. en el documento llamado “Guía buenas prácticas para almacenar documentos digitales”.

3.9.2 Gestión y disposición de medios removibles

Todos los dispositivos y unidades de almacenamiento removibles, tales como cintas, CD’s, DVD’s, dispositivos personales “USB”, discos duros externos, cámaras fotográficas, cámaras de video, celulares, entre otros, que se conecten a la red de datos de la ARN o que se encuentren bajo su custodia, están sujetos mediante las herramientas tecnológicas de control de la ARN, bajo las directrices de la Mesa de Seguridad.

Se debe hacer seguimiento a los medios de almacenamiento removibles como Discos Duros, Cintas, etc., con el fin de garantizar que la información sea transferida a otro medio antes de que esta quede inaccesible por deterioro o el desgaste que sufren a causa de su vida útil.

Se debe llevar el registro actualizado de todos los medios removibles de la ARN y deben estar almacenados en un ambiente seguro acorde con las especificaciones del fabricante.

Toda la información clasificada como PÚBLICA CONFIDENCIAL o PÚBLICA RESERVADA que sea almacenada en los diferentes activos de información, debe cumplir con las directrices de seguridad estipuladas para su protección definidas por el Grupo de Gestión documental y el documento TI-G-01 Guía de intercambio de información.

La Mesa de Seguridad puede restringir la conexión de medios de almacenamiento removibles a los equipos de cómputo que sean propiedad de la ARN o que estén bajo su custodia, y puede llevar a cabo cualquier acción de registro o restricción, con el fin de evitar fuga de información o infección por malware a través de medios removibles.

3.9.3 Borrado seguro

Todos los medios de almacenamiento que sean de propiedad de terceros para su uso dentro de la red interna deben ser autorizados por la ARN.

Todos los medios de almacenamiento que contengan información de la ARN, que salgan de la Entidad y que no se vuelvan a utilizar para dicho fin, y aquellos equipos que sean o contengan medios de almacenamiento que vayan a ser dados de baja deben seguir el procedimiento de borrado seguro definido por la ARN, el cual garantiza que la información no es recuperable (Aplica para medios de almacenamiento, equipos en arriendo, equipos de proveedores, discos duros externos, etc.).

3.9.4 Transferencia de medios físicos

Toda la información clasificada como PÚBLICA CONFIDENCIAL o PÚBLICA RESERVADA que se almacene en medios removibles y que sean transportados fuera de las instalaciones de la ARN, debe cumplir con las disposiciones de seguridad indicadas en el documento TI-G-01 Guía de Intercambio de Información publicada en SIGER.

El transporte de los medios físicos se debe hacer mediante un medio de transporte confiable y seguro, tomando las medidas y precauciones necesarias para garantizar que los medios de almacenamiento sean transportados adecuadamente, de esta forma evitar una afectación a la integridad, confidencialidad y disponibilidad de la información.

Se debe llevar un registro o cadena de custodia de los medios de almacenamiento físico que son transportados, de acuerdo con los lineamientos del Grupo de Gestión Documental y el Grupo de Almacén e inventarios.

3.9.5 Recomendaciones para el uso de la herramienta de OneDrive:

Al momento de realizar el proceso de cargue y/o consulta de los documentos por medio del navegador en línea, tenga en cuenta las siguientes restricciones durante el proceso:

- El manejo de la información debe realizarse de acuerdo con lo establecido en el numeral *3.8 Política del uso aceptable de los activos Regla No 4: del manejo de la información*.
- No está permitido el almacenamiento de información de propiedad de la ARN en servicios no licenciados o no autorizados.
- El tamaño máximo de los documentos es de 10 GB.
- Las carpetas y archivos no deben contener en sus nombres, caracteres especiales como: (/ \ : * ¿? “ >< | # % ~ & =)
- Tenga en cuenta que la longitud máxima para un nombre de archivo está entre 5 a 30 caracteres, controle la creación de carpetas y subcarpetas ya

que la ruta total del archivo suma las características de todos estos elementos y no debe exceder los 255 caracteres.

- Se prohíbe subir información personal como: fotos, videos, música en formatos MP3 y MP4, archivos con extensiones (.EXE), accesos directos, archivos del sistema (.DLL, .TMP).
- Si tiene archivos que contengan macros, filtros, combinación de correspondencia, se recomienda trabajar estos archivos de forma local y No en línea.
- La velocidad de trasferencia de la información no solamente depende del canal de Internet, sino de la cantidad de información y el procesamiento de la plataforma del proveedor Microsoft, la cual, no es exclusiva para la Entidad.
- La información PÚBLICA CONFIDENCIAL o PÚBLICA RESERVADA nunca debe reposar en carpetas en la nube (OneDrive) esta herramienta debe utilizarse exclusivamente para información transitoria o de forma colaborativa con otros empleados públicos o contratistas de la ARN.

3.10 POLÍTICA DE INTERCAMBIO DE INFORMACIÓN

La ARN propende por la protección de la información en el momento en que sea transferida o intercambiada de manera interna o con otras entidades y establece el documento TI-G-01 Guía de 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 seguras para llevar a cabo el intercambio de información digital y establece directrices para el intercambio de información en medio físico.

3.10.1 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.
- La ARN cuenta con una Guía para intercambio de información, en la cual se establecen las directrices mínimas tanto al interior de la entidad como con otras entidades, organizaciones o terceros.
- 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.

- La Oficina de Tecnologías de la Información dispone de herramientas de monitoreo para prevención de fuga de información desde los equipos de cómputo de los empleados públicos y contratistas, las cuales generan alertas con base en reglas predefinidas las cuales son revisadas periódicamente para tomar las acciones pertinentes.
- La Oficina de Tecnologías de la Información habilita las herramientas necesarias para asegurar la transferencia de información al interior y exterior de la ARN, contra interceptación, copiado, modificación, direccionamiento y destrucción.
- La Oficina de Tecnologías de la Información, debe controlar las acciones para envío automático de correo electrónico a direcciones de correo externo.
- La Oficina de Tecnologías de la Información, realiza el control del uso de sistemas de transferencia de archivos a través de FTP, los cuales deben realizarse estableciendo una Virtual Protocol Network (VPN) o Web Services y en tal caso se debe garantizar que se utilice protocolo seguro HTTPS.
- 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.

3.11 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 empleados públicos y contratistas, 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, tales son:

- Como parte de las condiciones iniciales de ingreso, todo empleado público, firma 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 empleados públicos y contratistas deben contar con una inducción o transferencia de conocimiento 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

empleado público o contratista durante la vigencia de su vinculación o en desarrollo de sus obligaciones contractuales, son propiedad de la ARN.

- Es responsabilidad de cada empleado público y contratista 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) empleados públicos y contratista(es) delegado(s) en los sistemas de información correspondientes a través de la mesa de ayuda.
- Los empleados públicos y contratistas a los cuales se les autoriza trabajo en casa deben seguir los lineamientos que se establezcan desde Talento Humano y para el caso de Teletrabajo deben cumplir con lo establecido en el TH-M-01 - Manual de Teletrabajo y continuar aplicando las buenas prácticas de seguridad de la entidad.

3.12 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 el funcionamiento correcto y seguro.

3.12.1 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 debe tener en cuenta las siguientes disposiciones:

    - Se debe contar con verificación de las páginas web para comprobar la presencia de códigos maliciosos.
    - Ningún empleado público y contratista puede ejercer actividades de administración sobre su equipo. Los únicos autorizados para desarrollar

esta función es el personal 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 realiza sensibilización al a los empleados públicos y contratistas sobre la protección contra software malicioso y buenas prácticas de seguridad informática.

3.12.2 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 efectúa 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 tiene 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 puede 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 el personal 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 obtienen del backup mensual o en su defecto del último respaldo realizado.

- Los empleados públicos y contratistas son responsables de la información almacenada en el equipo asignado y serán los encargados de mantener copias de respaldo de sus archivos, y la información debe ser entregada al supervisor del contrato o jefe inmediato al finalizar su vinculación. En caso de que se requiera una copia de respaldo de la información, lo pueden solicitar a la Oficina de Tecnologías de la Información a través de la Mesa de Servicios a la extensión 10999 o al correo soporte@reincorporacion.gov.co.

3.12.3 Gestión de seguridad en redes

- Se debe 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 debe ser registrada y monitoreada a fin de detectar y controlar situaciones anómalas.
- Se debe implementar la independencia de la red para empleados públicos y contratistas ~~y~~ de la de invitados.

3.12.4 Gestión de comunicaciones masivas

Para la realización de transmisiones en vivo del Director General de la ARN donde se busque la interacción con un elevado número de ciudadanos se permite coordinar con la Oficina Asesora de Comunicaciones la realización de la transmisión a través de la fan page de la ARN en Facebook o la que determine la Mesa de Seguridad de la Información.

3.13 POLÍTICA DE CONTROL DE ACCESO

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

3.13.1 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 empleado público y contratista 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 empleado público y contratista finaliza su relación laboral, sus permisos de acceso debe 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.

3.13.2 De los Sistemas de Información

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

Todos los desarrollos de sistemas de información deben regirse de acuerdo con los lineamientos de la Oficina de Tecnologías de la Información.

3.13.3 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 empleados públicos y contratistas no deben revelar estas a terceros ni utilizar claves ajenas.
- Todo empleado público y contratista 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 tres (3) 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 empleado público y contratista 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 deben 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 deben atender el plan de preservación digital vigente.
- En caso de que la cuenta de usuario se encuentre involucrada en algún delito informático o delito penal, será responsabilidad solo del empleado público y contratista que tenga asignada esta cuenta.

3.13.4 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 empleado público y contratista, 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.
- Todo empleado público y contratista debe 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.

3.14 POLÍTICA DE PANTALLA Y ESCRITORIO LIMPIO

3.14.1 Ubicación y protección de equipos de cómputo e impresoras

- El área de trabajo de los empleados públicos y contratistas 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.

3.14.2 Equipo desatendido por el empleado público o contratista

- Toda vez que el empleado público o contratista 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.

3.15 POLÍTICA DE PROTECCIÓN DE DISPOSITIVO PROPIO (BYOD)

La ARN define las medidas necesarias para evitar que la información pública reservada o pública clasificada se vea comprometida en su integridad y confidencialidad al ser almacenada en dispositivos de propiedad de empleados públicos y/o contratistas de la ARN.

Esta política aplica a todos los dispositivos electrónicos personales tales como teléfonos inteligentes y tabletas, los computadores portátiles que no pertenecen a la Entidad pero que son utilizados por los empleados públicos y/o contratistas para acceder o almacenar información. A estos dispositivos se les conoce comúnmente dentro del área de seguridad informática como BYOD (Bring Your Own Device).

La ARN a través de la Mesa de Seguridad de la Información define en qué momento se considera viable autorizar el uso de dispositivos personales que no sean propiedad de la Entidad para el tratamiento de la información institucional.

3.15.1 Responsabilidades

- Los responsables de los procesos de la ARN deben determinar bajo qué circunstancias se autoriza el uso de dispositivos que no pertenecen a la entidad (BYOD) para almacenar o procesar información pública reservada o información pública clasificada, así como la aplicación de las políticas de seguridad requeridas para la información que se almacene y gestione en el dispositivo personal del empleado público y/o contratista.
- Los responsables de los procesos deben evaluar los riesgos asociados a la divulgación de información pública reservada o información pública clasificada antes de autorizar el uso de los BYOD.
- El empleado público y/o contratista al que se autorice un BYOD debe garantizar bajo acta de compromiso de confidencialidad que la información pública reservada o información pública clasificada correspondiente a sus labores asignadas será almacenada de manera temporal y eliminada del dispositivo una vez procesada.
- Todo dispositivo BYOD autorizado para almacenar información de la entidad debe cumplir con la reglamentación vigente en materia de uso de software legal. El usuario es enteramente responsable de contar con todo el software de su dispositivo debidamente licenciado, así como la configuración de cualquier aplicación en el dispositivo.

- Las soluciones tecnológicas implementadas por la ARN facilitan el uso de escritorio remoto a sus equipos asignados por la Entidad para que los empleados públicos y contratistas tengan acceso de forma que se evite el almacenamiento de información institucional en equipos que no son propiedad de la ARN. En este sentido, los equipos BYOD deben contar con las aplicaciones que permitan dicho acceso.
- El propietario del dispositivo BYOD debe aplicar todas las medidas de seguridad que estén a su alcance para preservar la integridad, confidencialidad y disponibilidad de la información que se encuentre en su dispositivo personal.
- Los empleados públicos y/o contratistas deben mantener actualizado el sistema operativo y todas las aplicaciones de los dispositivos móviles.
- Configurar el bloqueo automático del equipo tras un breve periodo de inactividad.
- El desbloqueo debe realizarse mediante contraseña, patrón de desbloqueo o por medios biométricos.
- Para teléfonos inteligentes y tabletas, se requiere que las aplicaciones de correo electrónico institucional y mensajería instantánea deben contar con una herramienta que permita el bloqueo de aplicaciones a través de una contraseña.
- El propietario del dispositivo debe informar a la mayor brevedad a la Mesa de Servicios, y a la autoridad competente el robo o pérdida de su dispositivo.
- La ARN podrá orientar a los empleados públicos y contratistas sobre la instalación de las soluciones en sus equipos. En ningún caso se podrá hacer responsable de los daños que se puedan causar en los equipos personales, ni podrán dar soporte técnico a equipos que no son propiedad de la Entidad.
- Los empleados públicos y contratistas deberán propender por utilizar los canales, las herramientas y repositorios que se encuentran disponibles por la Entidad, para ubicar la información institucional y registrar su gestión.

3.16 POLÍTICA PARA USO DE DISPOSITIVOS MÓVILES

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

- Instalar un antivirus en el dispositivo móvil.

- 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.

3.17 POLÍTICAS DE CRIPTOGRAFÍA

3.17.1 Política de controles criptográficos

La ARN vela 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.

La ARN implementa el uso herramientas y técnicas criptográficas, con el fin de fortalecer la seguridad de la información.

Todo sistema de información o servicio tecnológico debe incluir parámetros de seguridad basado en usuarios, perfiles y roles, para ser aplicados en la autorización y autenticación según las necesidades.

Se utilizarán controles criptográficos en los siguientes casos:

- Para la transmisión de información Reservada o Clasificada, fuera de la Entidad.
- En la protección de la información a resguardar, cuando así lo establezca el Mesa de Seguridad de la Información, el generador de la información o el Oficial de Seguridad de la Información.
- Para todos los equipos de cómputo en las unidades de disco físicas.

- Para unidades de almacenamiento externo.

3.17.2 Normas de controles criptográficos

- El sistema de mensajería instantánea debe cumplir con los requerimientos criptográficos del standard federal de procesamiento de información FIPS 140-2.
- Los propietarios de los activos de información y los responsables de su tratamiento deben 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 provee las herramientas de cifrado 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 evalúa la implementación de métodos para cifrar la información reservada o restringida, teniendo en cuenta el impacto que tenga respecto al rendimiento de dichos sistemas.

3.18 POLÍTICA DE RELACIÓN CON PROVEEDORES

La ARN establece 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.

3.19 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 y gestiona su remediación.

3.19.1 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 un ente independiente al área objeto de las pruebas, con el fin de garantizar la independencia y 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 o minimizar la exposición al riesgo de estos.
- Revisar, valorar y gestionar las vulnerabilidades técnicas encontradas, apoyándose en herramientas tecnológicas para su identificación.
- Generar y ejecutar o monitorear los planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica.

3.20 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 que 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 el Plan de Continuidad del Negocio (BCP - Business Continuity Plan).

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.
- La Oficina de Tecnologías de la Información apoya en la identificación de los ciberactivos críticos con base en los activos críticos definidos en el análisis de impacto en el negocio (BIA- Business Impact Analysis). Estos ciberactivos son aquellos que contienen, trasmiten o procesan información de los servicios esenciales para la ARN.

ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DEL NEGOCIO

A continuación, se indican una serie de buena practicas con el fin de preservar la confidencialidad, integridad y disponibilidad de la información en escenarios de continuidad del negocio.

Buenas prácticas de ciberseguridad para trabajo en casa y teletrabajo.

Con el fin de proteger la información institucional de la ARN ante las amenazas de internet se recomienda lo siguiente:

- Seguir los procedimientos que se establezcan por las Directivas de la entidad.
- Hacer uso de los recursos tecnológicos suministrados por la ARN, en caso de presentar daño debe reportarlo inmediatamente a la Mesa de servicios a través de la extensión 10999, correo electrónico: soporte@reincorporacion.gov.co y no manipularlo o abrirlo.

- Evitar utilizar conexiones wifi gratuitas disponibles en diferentes establecimientos debido a que se pueden comprometer contraseñas, usuarios e información sensible de la entidad.
- Al utilizar la conexión a través de VPN configurar el usuario brindado por la entidad y evitar compartir las credenciales.
- Usar únicamente las herramientas corporativas autorizadas por la ARN para los ambientes colaborativos institucionales como Microsoft Teams.
- Evitar el uso de herramientas colaborativas no autorizadas ni licenciadas.
- Reportar a la mesa de servicio si recibe un correo, mensaje de texto o cadena de WhatsApp sospechosos, evite abrir o compartir.
- Si está trabajando con información de la entidad, al retirarse del equipo asegúrese de que éste quede bloqueado (tecla Windows + L) para evitar la manipulación o pérdida de información por parte desconocidos, familiares o niños.
- Sea precavido con los datos que comparte a través de medios digitales y telefónicos como: nombres, correo electrónico, número de celular, cuentas bancarias entre otros.
- Establecer horarios de cierre de sesión para conexiones en los sistemas de la entidad ya que permitir que las conexiones remotas permanezcan abiertas indefinidamente aumenta la ventana de disponibilidad para el acceso NO autorizado.
- Si está trabajando en un equipo personal, guarde los documentos de la Entidad en los medios dispuestos por la ARN como **carpetas compartidas y/o carpetas de trabajo.**
- Si sospecha o detecta un incidente de seguridad de la información reportar a la Mesa de servicios a través de los canales de comunicación establecidos.

II. DE LA PROTECCIÓN DE DATOS PERSONALES

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, propende 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.

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

La ARN da cumplimiento a la normatividad legal vigente que dicte disposiciones para la protección de datos personales teniendo en cuenta lo descrito en el documento DE-M-06 Manual de Protección de Datos publicado en SIGER.

III. DE LOS DERECHOS DE AUTOR

La ARN vela por el cumplimiento de la legislación y reglamentación vigente relacionada con la seguridad de la información, entre ella la referente a derechos de autor y propiedad intelectual para lo cual ha dispuesto el documento AJ-P-12 procedimiento para el registro de propiedad intelectual.

1. GENERALIDADES

Las obras que resulten del ejercicio de las funciones de los empleados públicos o en el cumplimiento de obligaciones contractuales por parte de los contratistas de la entidad, en el marco de una vinculación legal y reglamentaria se tendrán por autor a la persona natural que las creó, quien conserva las prerrogativas de índole moral, pero la entidad estatal será quien ostente los derechos patrimoniales; es decir, la facultad de explotar libremente las obras y autorizar su utilización por parte de terceras personas. lo anterior de conformidad a lo establecido en el artículo 91 de la Ley 23 de 1982.

2. ASIGNACIÓN DE RESPONSABILIDADES

- Todos los empleados públicos o contratistas de la ARN deben velar por el cumplimiento de normas de derechos de autor y derechos conexos.
- Todos los empleados públicos, contratistas o terceros que hacen uso de la plataforma tecnológica de la Entidad solo pueden utilizar software autorizado por la Oficina de Tecnologías de la Información.
- La Oficina Asesora Jurídica apoya el registro de los Derechos de Autor cuando corresponda.

3. REGISTRO ANTE LA DIRECCIÓN NACIONAL DE DERECHO DE AUTOR

La entidad a cargo de proteger, promover y defender el derecho de autor y los derechos conexos en el país es la Dirección Nacional de Derecho de Autor, DNDA.

Por ello el Registro Nacional de Derecho de Autor se lleva a cabo en la Oficina de Registro de la Unidad Administrativa Especial de la DNDA de acuerdo con las competencias asignadas.

4. REGISTRO DE SOFTWARE O SOPORTE LÓGICO[1]

De un software se pueden registrar cualquiera de los siguientes 3 elementos: Su documentación completa, el código fuente o su manual de usuario.

La ARN debe escoger cualquiera de ellos, o registrar los 3 en caso de que desee un registro más completo.

En caso de entregar material en formato electrónico, debe ser en medio óptico para una mejor conservación.

No se debe entregar material publicitario, se debe entregar la documentación que permita identificar correctamente el software y sus características más importantes.

Las páginas web, no son objeto de registro, así como tampoco es protegible su objetivo (función o concepto). Sin embargo, los elementos individualmente considerados que estén presentes en la página web y que puedan ser considerados una obra literaria o artística, podrán registrarse individualmente en su respectiva categoría.

Del mismo modo, será registrables, bien sea en la forma de un soporte lógico (software) o como una obra escrita (literaria), las bases de datos cuya selección o disposición de las materias que la conforman, constituyan una creación intelectual.

DOCUMENTOS DE REFERENCIA Y FUENTES DE INFORMACIÓN

- Manual de Gobierno Digital

[1] Dirección Nacional de derecho de autor (2018). Derecho de autor. Bogotá, Colombia. Recuperado de http://derechodeautor.gov.co/tutorial.

- Estándar ISO 27001 Versión 2013
- Políticas de tratamiento de la información personal en la Superintendencia de Industria y Comercio, www.sic.gov.co.
- Lineamientos de derechos de autor de la Dirección Nacional de derechos de autor, http://derechodeautor.gov.co/web/guest/home
- Manual de Seguridad de la Información de la Presidencia de la República.
- Política Nacional de Gestión Integral de Residuos de Aparatos Eléctricos y Electrónicos.