AGENCIA PARA LA REINCORPORACIÓN Y LA NORMALIZACIÓN

AGENCIA PARA LA REINCORPORACIÓN Y LA NORMALIZACIÓN (ARN)

MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C. DICIEMBRE DE 2023

TABLA DE CONTENIDO

1. OBJETIVO

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

2. 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.

3. 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 esta 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: Software de correspondencia - SIGOB, Software para la administración de la planeación y la gestión.

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.

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.

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.

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 esta 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.

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

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.

DOCUMENTO: Información registrada, cualquiera sea su forma o el medio utilizado (acuerdo 002 de 2014, AGN)

DOCUMENTO DE ARCHIVO: Registro de información producida o recibida por una persona o entidad en razón a sus actividades o funciones, que tiene valor administrativo, fiscal, legal, científico, histórico, técnico o cultural y debe ser objeto de conservación en el tiempo, con fines de consulta posterior. (Acuerdo 002 de 2014, AGN)

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

EAIS: Equipo de atención de Incidentes de Seguridad, se refiere al equipo especializado que se conforma para la atención del incidente de seguridad de la información. Este grupo estará conformado por el equipo de seguridad informática y redes, el Oficial de Seguridad de la Información de la ARN y el SOC)

ETIQUETADO: Conjunto adecuado de tareas para el rotulado y marcado de los activos de información de acuerdo con el esquema de clasificación adoptado por la ARN, alineado al cumplimiento de las diferentes normas.

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: Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen (artículo 6, literal a de la Ley 1712 de 2014). Lo que se constituye en 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: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal (artículo 6, literal b de la ley 1712 de 2014). Es aquella información que puede ser distribuida, entregada o publicada abiertamente al público sin que cause daño alguno a la entidad, a sus contratistas, otras dependencias o a otras entidades.

INFORMACIÓN PÚBLICA CLASIFICADA. Es aquella información que estando en poder o custodia de la ARN, en su calidad de propietario y/o responsable, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados (artículo 6, literal c, de la Ley 1712 de 2014). Esta información *contiene los* datos semiprivados, privados o sensibles *y* solo podrá divulgarse según las reglas establecidas en normas asociadas. (decreto 1081 de 2015: Articulo 2.1.1.4.1.1)

INFORMACIÓN PÚBLICA RESERVADA: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de calidad de propietario y/o responsable, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en la ley (artículo 6, literal d, de la Ley 1712 de 2014). Esta información es *reservada* por razones de defensa y seguridad nacional, seguridad pública o relaciones internacionales*, los derechos de la infancia y la adolescencia, entre otros*. *(*decreto 1081 de 2015: Articulo 2.1.1.4.2.1*)*

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 DE LA INFORMACIÓN: 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 de la Información no suplanta las responsabilidades asignadas al Oficial de Seguridad de la Información, al Oficial 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.

ONEDRIVE: 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.

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.

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.

SHAREPOINT ONLINE: Herramienta colaborativa de Microsoft 365 que permite almacenar, organizar y compartir información desde cualquier dispositivo seguro.

SIG: Sistema Integrado de Gestión

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 y reincorporación – SIRR.

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.

TELETRABAJO: Es una forma de organización laboral, que se efectúa en el marco de un contrato de trabajo o de una relación laboral dependiente, que consiste en el desempeño de actividades remuneradas utilizando como soporte las tecnologías de la información y la comunicación (TIC) para el contacto entre el trabajador y empleador sin requerirse la presencia física del trabajador en un sitio específico de trabajo
La modalidad de Teletrabajo adoptada por la Agencia para la Reincorporación y la Normalización es Suplementaria, a través de la cual los empleados públicos desarrollan sus actividades algunos días de la semana en el lugar de residencia reportado y el resto de tiempo en las instalaciones de la Entidad

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

TRABAJO EN CASA: Se entiende como trabajo en casa la habilitación al empleado público para desempeñar transitoriamente sus funciones o actividades laborales por fuera del sitio donde habitualmente las realiza, sin modificar la naturaleza del contrato o relación laboral, o legal y reglamentaria respectiva, ni tampoco desmejorar las condiciones del contrato laboral, cuando se presenten circunstancias ocasionales, excepcionales o especiales que impidan que el trabajador pueda realizar sus funciones en su lugar de trabajo, privilegiando el uso de las tecnologías de la información y las comunicaciones.

TRABAJO REMOTO: Es una forma de ejecución del contrato de trabajo en la cual toda la relación laboral, desde su inicio hasta su terminación, se debe realizar de manera remota mediante la utilización de tecnologías de la información y las telecomunicaciones u otro medio o mecanismo, donde el empleador y trabajador, no interactúan físicamente a lo largo de la vinculación contractual. En todo caso, esta forma de ejecución no comparte los elementos constitutivos y regulados para el teletrabajo y/o trabajo en casa y las normas que lo modifiquen.

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.

4. CONSIDERACIONES GENERALES

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, por tanto, es responsabilidad de todos los empleados públicos, contratistas y terceros el cumplimiento de cada una de estas políticas y lineamientos, acorde con la normatividad vigente.

4.1 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 el software para la administración de la planeación y la gestión, entre otros los siguientes manuales: DE- M-02 Manual de gestión del riesgo, DE-M-11 Manual del sistema integrado de gestión - SIG, DE-M-05 Manual para la gestión de proyectos, TH-M-01 Manual de teletrabajo suplementario, AC-M-01 Manual del sistema de peticiones, quejas, reclamos, sugerencias y denuncias - PQRS-D, GA-M-01 Manual de seguridad preventiva, GA-M-02 Manual para el manejo y control administrativo de bienes de la entidad,CO-M-01 Manual de operación proceso de gestión de comunicaciones, GD-M-02 Manual para la producción de documentos, DE-M-06 Manual de Protección de Datos, BS-M-01 Manual de contratación, supervisión e interventoría, AJ-P-12 Procedimiento para la inscripción de propiedad intelectual. EM-M-01 Manual de auditoría interna.

4.2 CONTROLES DE LA DOCUMENTACIÓN DEL SGSI

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

4.3 REVISIÓN

El Manual del Sistema de Gestión 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 Oficial de Seguridad de la Información y la Mesa de Seguridad de la Información. La actualización y aprobación del documento se realizan de acuerdo con lo definido en lo métodos de operación establecidos en el SIG para tal fin, GD-M-02 Manual para la producción, GD-P-04 Procedimiento control de documentos

4.4 ACCIONES POR INCUMPLIMIENTO DE LAS POLÍTICAS DEL SGSI

Para los empleados públicos que llegaren a verse involucrados en alguna violación de la Política de Seguridad de la Información, la secretaria general adelantará las acciones necesarias teniendo en cuenta lo dispuesto en la Ley 1952 de 2020- Código General Disciplinario. Para los contratistas la secretaria general adelantará las acciones a las que haya lugar.

5. CONTENIDO Y DESARROLLO

5.1 DE LA SEGURIDAD DE LA INFORMACIÓN

5.1.1 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 entidad el cual debe ser adoptado por la alta dirección, empleados públicos, contratistas y demás partes interesadas en razón al cumplimiento de la misión de la entidad, que incluyen aspectos relacionados con compartir, validar, recolectar, procesar, intercambiar o consultar información. Así mismo, el SGSI aplica a toda la información creada, procesada o utilizada por la entidad, sin importar el medio, sea físico o digital donde ésta se encuentre. El SGSI está incorporado dentro del Sistema Integrado de Gestión y es responsable de su adopción el Director General de la ARN.

5.1.2 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.

5.1.2.1 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 en lo correspondiente a la implementación, gestión y seguimiento del Modelo Integrado de Planeación y Gestión - MIPG, interviene para la adecuada dirección, implementación, implantación, gestión y mantenimiento del SGSI y de la Política de Gobierno Digital y la política de Seguridad Digital en la ARN. En el marco del cual se creó una Mesa de trabajo de Seguridad de la Información como un órgano operativo y de apoyo para la asesoría y coordinación de los diferentes temas

relativos a la seguridad de la infraestructura física, de los empleados públicos y contratistas, de la información misional que puedan afectar la confidencialidad, integridad y disponibilidad de la Información en 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.

En relación con la Mesa de Seguridad de la Información, en el numeral 8 del presente documento se relacionan los integrantes, sus funciones y los lineamientos para su operación.

5.1.2.2 ASIGNACIÓN DE RESPONSABILIDADES

- **El Comité Institucional de Gestión y Desempeño es el responsable de**:

  Asegurar la Implementación y Desarrollo de las Políticas de Gestión y Directrices en materia de Seguridad Digital y de la Información, de conformidad con la normatividad vigente y aplicable.

- La Mesa de Seguridad de la Información 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

- **Coordinador de la Mesa de Seguridad de la Información**:

El Jefe de Oficina de Tecnologías de la Información quien lidera la Política de Seguridad Digital, delega al Oficial de Seguridad de la Información la coordinación de las funciones de la respectiva Mesa, para lo cual la ARN destinará recursos que apoyen el desarrollo de las siguientes actividades a su cargo:

- ✓ Coordinar la realización de la mesa de seguridad de la información proponiendo directrices y acciones que permitan la implementación, seguimiento y mejoramiento del sistema de gestión de seguridad de la información, apoyando su desempeño en el marco del sistema integrado de gestión de la Entidad.
- ✓ Liderar con los responsables de los procesos en la implementación, seguimiento, cambios y mejoramiento de las directrices de seguridad, identifi8uu8cación de riesgos, asesoría en aplicación de metodología de gestión de riesgos, y acciones orientadas al cumplimiento del sistema de gestión de seguridad de la información.

- ✓ Articular las acciones encaminadas a la gestión de activos de información y responsabilidad demostrada en concordancia con la oficina asesora de planeación en el marco del sistema integrado de gestión; validando el tratamiento de riesgos, amenazas o vulnerabilidades en los activos, y monitoreando cambios significativos sobre los mismos.
- ✓ Diseñar, proponer y acompañar la implementación de políticas, lineamientos y recomendaciones de interoperabilidad para el intercambio seguro de información interno y externo en la entidad.
- ✓ Participar en los programas, planes, proyectos y actividades requeridas en el componente transversal de seguridad de la información asociados al plan de transformación digital y el Plan Estratégico de Tecnologías de la Información - PETI de la Entidad.
- ✓ Presentar a la mesa de seguridad de la información informes de métricas, controles e iniciativas del estado de seguridad de la información de la entidad; así como el seguimiento y verificación al plan de continuidad de negocio de la entidad liderado por la subdirección administrativa, y actividades asociadas al proyecto DLP (DATA LOSS PREVENTION) de la ARN, con el propósito de evitar la fuga de información.
- ✓ Acompañar e implementar medidas sobre la gestión de activos de información por parte de las dependencias para el control de la información clasificada y reservada en la ARN y la articulación a través de la oficina asesora de planeación de los instrumentos de información pública y demás fuentes de información.
- ✓ Realizar seguimiento a la respuesta a incidentes, así como, la investigación de las violaciones de la seguridad informática y las relacionadas con la información, incluyendo los relacionados con información personal que sean de su conocimiento, que permitan el soporte y asesoría dentro las investigaciones disciplinarias y legales necesarias.
- ✓ Apoyar la identificación de las necesidades e implementación de estrategias de difusión, sensibilización, capacitación y entrenamiento, que permitan fortalecer las capacidades de seguridad de la información.
- ✓ Apoyar la respuesta a consultas de información, requerimientos y demás comunicaciones internas y externas.
- ✓ Ejercer la secretaría técnica de la mesa de seguridad de la información, documentando su gestión mediante actas, informes, documentos de seguimiento y complementarios.

- **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 responsable de seguridad Informática pueda desarrollar las responsabilidades a su cargo:

- ✓ Elaborar, documentar, actualizar, monitorear y hacer seguimiento al Plan del Sistema de Gestión de Seguridad y Protección de la Información y gestión de riesgos que incluye la revisión y evaluación periódica de las políticas de seguridad informática y de seguridad de la información y sugerir a la Mesa de Seguridad de la Información y al Oficial de Seguridad de la Información los cambios necesarios.
- ✓ Investigar y proponer estrategias, políticas, lineamientos, estándares, proyectos y actividades de soluciones informáticas en temas relacionados con la Gestión de Seguridad y Protección y gestión de riesgos de la Información, que incluye. monitorear la ocurrencia de violaciones de seguridad y aplicar acciones correctivas para asegurar que se provea la seguridad adecuada
- ✓ Planear, ejecutar, administrar, gestionar, monitorear, evaluar y hacer seguimiento a las plataformas tecnológicas de seguridad, monitoreo de tráfico, acceso y gestión de eventos de seguridad de la ARN.
- ✓ Promover la aplicación de metodologías y estándares de la industria de TICs en el proceso de diseño, implementación y soporte de los servicios tecnológicos a su cargo, que incluye 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; realizar las recomendaciones, monitorear y verificar su aplicación y 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.
- ✓ Participar en la adquisición, contratación y supervisión de bienes y/o servicios de tecnologías de la información y comunicación de datos, en los aspectos técnicos de los procesos contractuales según las necesidades detectadas, y brindar las recomendaciones en los temas de seguridad y protección de la información y gestión de riesgos informáticos, que incluye 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
- ✓ Elaborar, implementar y realizar pruebas de planes de contingencia que aseguren la disponibilidad de los servicios tecnológicos y sistemas de información de la Entidad, que incluye probar la arquitectura de seguridad

para evaluar la fortaleza de la seguridad y para detectar y actuar ante las posibles amenazas.

- ✓ Coordinar con el Grupo de Sistemas de Información y demás dependencias la articulación para la seguridad y protección de la información y gestión de riesgos informáticos para afianzar su disponibilidad, integridad y confiabilidad tanto en el sistema de información y demás aplicativos misionales y de apoyo de la Entidad, que incluye preparar y monitorear el programa de sensibilización en seguridad informática para todo los empleados públicos y contratistas.

5.1.2.3 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 propende 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 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 de la Información, 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 o la directora(a) General, el Secretario General, el Director Programático, 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 a 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, eventos sospechosos y el mal uso de los recursos que identifiquen. 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 para empleados públicos en caso de incurrir en el incumplimiento de alguna de las normas estipuladas en el Sistema de Gestión de Seguridad de la Información. En el caso de contratistas se adelanta un proceso de

incumplimiento de acuerdo con los lineamientos del Grupo de Gestión Contractual.

- ✓ 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, deben iniciar el cambio de contraseña y comunicar éste u otros incidentes de seguridad de la información al Centro 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 para los empleados públicos o por los supervisores para los contratistas.

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 del sistema de información, aplicación o infraestructura de TI bajo su responsabilidad tanto en el proceso como en la utilización de este.
- ✓ Responder los requerimientos del centro 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 al centro de servicios los incidentes que detecte en la información 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 del 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 al líder funcional en la operación y manejo de los sistemas de información/aplicaciones y servicios de TI bajo su responsabilidad.

- **Líder de servicio**: Es el encargado desde el punto de vista de servicio tecnológico de 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 del Centro de Servicios y de 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.

5.1.2.4 De las autoridades frente al SGSI

Las modificaciones que impacten la política general del SGSI, será aprobada por el Comité Institucional de Gestión y Desempeño en el espacio de revisión por la Dirección.

Así mismo, las políticas específicas del Manual del Sistema de Gestión de Seguridad de la Información se aprueban en la Mesa de Seguridad de la Información.

Lo anterior, se evidencia en las siguientes instancias:

Primera instancia	Segunda Instancia	Tercera Instancia
Oficial de Seguridad de la Información	Mesa de Seguridad de la Información.	Comité Institucional de Gestión y Desempeño

NOTA: Las modificaciones son presentadas por el Oficial de Seguridad de la Información ante la Mesa de Seguridad con el propósito de contar con el aval de los integrantes de la mesa, así mismo, posterior al proceso de publicación en SAPYG el jefe de la Oficina de Tecnologías de la Información comunica al Comité Institucional de Gestión y Desempeño los cambios que han surgido en el SGSI.

El Equipo de atención de Incidentes de Seguridad – EAIS es la autoridad en primera instancia, para coordinar las acciones pertinentes para la gestión de incidentes de seguridad de acuerdo con lo descrito en los documentos TI- G-04 Guía para la gestión de incidentes de seguridad y el procedimiento TI-P-03 gestión de incidentes de seguridad.

5.1.3 POLÍTICAS

5.1.3.1 Política del Sistema de Gestión de Seguridad de la Información

La Agencia para la Reincorporación y la Normalización adopta el Sistema de Gestión de Seguridad de la información-SGSI, para lo cual se compromete con el cumplimiento de la confidencialidad, integridad, disponibilidad de la información institucional relacionada con su misión y visión mediante la gestión de riesgos, la cultura organizacional y la implementación de controles para dar cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua y al desempeño del SGSI.

5.1.3.2 Objetivos de SGSI

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

cumplimiento de los principios de confidencialidad, integridad y disponibilidad de la información.

5.1.3.3 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 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, el Grupo de Control Interno de Gestión.

5.1.3.4 Gestión del riesgo de seguridad digital

La ARN propende por el uso responsable del entorno digital teniendo en cuenta las directrices de los CONPES 3854 DE 2016 y CONPES 3995 DE 2020, 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 Informática de la Oficina de Tecnologías de la Información.

5.1.3.5 Políticas de planeación estratégica de tecnologías de la información

- **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.

- **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 de información deben ser solicitados a través del Centro 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.

- **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 del Centro 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, Talento Humano y el Grupo 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.

5.1.3.6 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, funciones u obligaciones contractuales:

- El uso de los activos de información que utiliza la ARN bien sea propio de la entidad o en arriendo, deben emplearse exclusivamente con propósitos laborales.
- La ARN proporciona a los empleados públicos y contratistas según las necesidades institucionales los equipos de cómputo y los programas instalados en ellos, así mismo, la Oficina de Tecnologías de la Información como parte de los controles técnicos de seguridad informática bloquea el acceso por USB a los equipos de cómputo propiedad de la entidad. En caso de requerir su habilitación temporal debe realizarse la solicitud a través del Centro de Servicios diligenciando el formato TI-F-01 Solicitud de usuario y/o recursos tecnológicos dispuesto en SAPYG.
- 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 solicitar autorización a su jefe inmediato para empleados públicos o al supervisor para el caso de contratistas 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 deben dar cumplimiento a 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 del Sistema de Gestión de Seguridad de la Información.
- Todo los empleados públicos y contratistas deben cumplir el 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 obligaciones contractuales. 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 Información, 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, 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 documento GA-M-02 Manual para el manejo y control administrativo de bienes 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.

El Grupo de Gestion Documental mediante la implementación de instrumentos archivísticos como la Tabla de Retención Documental, Programa de Gestion de Documentos Electrónicos de Archivo y la Tabla de Control de Acceso contribuye a la seguridad de la información aplicando los principios de confidencialidad, integridad y disponibilidad para la información de la ARN.

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.

- **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.

5.1.3.7 Clasificación de la información

La ARN clasifica la información con la participación de los propietarios, usuarios finales y custodios, 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 clasificar la información según el nivel de riesgo que genera su compromiso.

Para la clasificación de la información, la ARN adopta el modelo de clasificación el cual cubre 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 27001:2013) de acuerdo con los lineamientos descritos en el documento GD-I-08 instructivo de clasificación y etiquetado de la información.

5.1.3.8 Política del uso aceptable de los activos

Todo los empleados públicos y contratistas que hagan uso de los activos de información 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 de los empleados

públicos y obligaciones contractuales para los contratistas, por lo tanto, su utilización debe observar y cumplir las directrices que a continuación se relacionan:

- ✓ El acceso a internet se encuentra definido a través de perfiles de navegación de acuerdo con las necesidades institucionales de los grupos de trabajo articulado con las funciones u obligaciones contractuales de los empleados públicos y contratistas según lo autorice la Oficina de Tecnologías de la Información.
- ✓ El uso del servicio de internet está limitado exclusivamente para propósitos institucionales.
- ✓ 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 u obligaciones contractuales 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 de los empleados públicos y obligaciones contractuales de los 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 y debe ser solicitado a través del Centro de servicios.
- ✓ 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 empleados públicos o contratistas, 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 u obligaciones contractuales, 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 conservar y cuidar 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 el Grupo de Almacén e Inventarios en concordancia con 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 de cómputo propiedad de la ARN debe ser reportado al centro de servicios 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 CLASIFICADA 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 CLASIFICADA 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 CLASIFICADA 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.
- ✓ Talento Humano se encargará de tramitar la firma de la Autorización de uso de información personal para fines institucionales – empleados públicos y guardar las evidencias correspondientes.
- ✓ El Grupo de Gestión Contractual se encarga de tramitar la firma de la Autorización de uso de información personal para fines institucionales – contratistas y que repose una copia en la carpeta de contrato.
- ✓ El Grupo de Gestión Contractual en conjunto con los supervisores de contratos se encargan de tramitar la solicitud de información de contratistas (Personas jurídicas), que realizan tratamiento de datos personales sobre el cumplimiento de la Ley de Protección de Datos Personales y sus decretos reglamentarios y debe reposar copia en la carpeta contractual.

5.1.3.9 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

recursos de almacenamiento los cuales son: carpetas compartidas, SharePoint y OneDrive.

El manejo de la información debe realizarse de acuerdo con lo establecido en este documento en el numeral 5.1.3.8 Política del uso aceptable de los activos Regla No 4: del manejo de la información.

- **De las carpetas compartidas**

La OTI pone a disposición de los empleados públicos y contratistas la opción de acceder a las Carpetas de Trabajo o Workfolders en los equipos de cómputo propiedad de la entidad, ya sea a través de conexiones seguras por VPN / Escritorio Remoto o directamente en los dispositivos asignados. Así mismo, para determinados perfiles de usuarios la OTI adelanta pruebas de concepto para servicios de escritorios virtuales los cuales pueden ser accedidos desde un equipo de cómputo propendiendo por los accesos controlados a las plataformas tecnológicas de la Entidad.

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.

La OTI ha definido el servicio de copia de respaldo de usuario final (DLO) el cual realiza backup a la información almacenada en la carpeta denominada “Documentos” tales como pdf, Word, Excel, PowerPoint, txt, pst, zip y msg de los equipos de cómputo propiedad de la entidad asignados a los empleados públicos y contratistas los cuales son responsables del manejo de la información.

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 GD-M-05 Programa de gestión de documentos electrónicos de archivo.

Carpetas compartidas de apoyo

Las carpetas compartidas sobre la infraestructura ofrecida por la OTI serán administradas por las diferentes dependencias quienes deben dar un buen uso de la información y de la cuota de almacenamiento asignada 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 del Centro de Servicios por el Jefe de Dependencia o Coordinador, anexando el formato TI-F-01 Solicitud de Usuario y/o Recursos Tecnológicos dispuesto en SAPYG.

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.

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.

Carpetas compartidas de archivos de gestión electrónicos

Las carpetas compartidas de los archivos de gestión electrónicos, estructuradas por el Grupo de Gestión Documental con la infraestructura ofrecida por la OTI, se establecen con el propósito de almacenar, conformar y preservar los archivos electrónicos de archivo, los cuales deben dar cumplimiento a lo establecido en la

Guía para la Administración y Gestión de Carpetas Compartidas de Archivos Electrónicos GD-G-02. y con las Tablas de Retención Documental.

El acceso y administración de esta estructura de carpetas se encuentran bajo el coordinador de cada Unidad Administrativa, Grupo Interno de Trabajo y Grupos Territoriales, con apoyo de los responsables de gestión documental. De igual manera las solicitudes de permiso de lectura y escritura se encuentran estructurada con una línea de autorizaciones que inicia por solicitud del jefe inmediato y/o coordinador y finaliza con la consolidación y tramite de estas solicitudes por parte del Grupo de Gestión Documental, hacia el centro de servicios tecnológicos administrado por la OTI.

Este lineamiento se encuentra enmarcado como parte de las estrategias dispuestas dentro del Plan Estratégico de Tecnologías de la Información – PETI, y los subprogramas de instrumentos archivísticos tales como el Plan institucional de archivo- PINAR y Programa de Gestión Documental - PGD.

- **Gestión y disposición de medios removibles**

Todos los dispositivos y unidades de almacenamiento removibles, tales como, CD’s, DVD’s, dispositivos “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 de la Información.

Se debe hacer seguimiento a los medios de almacenamiento removibles como Discos Duros, dispositivos “USB”, 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.

Toda la información clasificada como PÚBLICA CLASIFICADA 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 de la Información 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.

- **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 los lineamientos de borrado seguro, el cual garantiza que la información no es recuperable (Aplica para medios de almacenamiento, equipos de cómputo, discos duros externos, etc.).

- **Transferencia de medios físicos**

Toda la información clasificada como PÚBLICA CLASIFICADA 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 el software para la administración de la planeación y la gestión.

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.

5.1.3.10 Política de uso de OneDrive y SharePoint Online

La política que se detalla a continuación regula el uso de las aplicaciones OneDrive® y SharePoint Online de Microsoft 365® por parte de empleados públicos y contratistas (en adelante LOS USUARIOS) de la ARN de acuerdo con las siguientes consideraciones:

- Está permitido el uso sólo a empleados públicos y contratistas activos de la ARN que además tengan vigente una cuenta de correo electrónico institucional del dominio @reincorporacion.gov.co. En caso de requerir acceso temporal para usuarios externos por necesidades institucionales se gestiona con la autorización del responsable del canal de SharePoint Online.

- La información institucional definitiva debe reposar en las carpetas compartidas las cuales están articuladas con el respaldo de información centralizada, en tal sentido OneDrive y SharePoint Online debe utilizarse exclusivamente para información transitoria o de forma colaborativa con otros empleados públicos o contratistas de la ARN.

- Los usuarios podrán almacenar documentos de trabajo (es decir. aquellos documentos o archivos que se requieren para el desarrollo normal de las actividades, funciones u obligaciones contractuales) y permitir el acceso a otros usuarios asignando roles de solo lectura o de edición según se requiera, evitando así, el envío de copias por correo electrónico.

- Cada usuario es responsable de la gestión de su espacio de OneDrive y de la documentación allí almacenada, así como, la asignación de permisos o privilegios de consulta y edición de los documentos, archivos o cualquier información que publique en OneDrive tanto con usuarios internos como externos.

- Es responsabilidad del usuario descargar en la carpeta compartida los archivos que se encuentran almacenados en OneDrive en caso de vacancia temporal, vacaciones, renuncia o retiro de la Entidad.

- El propietario del espacio de SharePoint Online es responsable de la administración del espacio y la asignación de miembros de equipo y acceso a la información y de la documentación allí almacenada.

- Los miembros de equipo e invitados del espacio de SharePoint Online son responsables de la gestión de la información allí almacenada, de acuerdo con los permisos que el propietario les haya asignado.

- Está prohibido almacenar, publicar, compartir y editar documentos que sean considerados como material ofensivo y no adecuado o que atente contra la integridad, dignidad, honra o características propias de la individualidad de los usuarios y también de personas o entidades externas.

- Cuando los usuarios requieran publicar, compartir o difundir información o documentos que estén catalogados, etiquetados o anunciados como **información pública clasificada y/o información pública reservada** deben segu**ir** lo indicado en el documento GD-I-08 Instructivo de clasificación y etiquetado de información, así mismo deben previamente establecer un convenio o acta de intención, cifrar la información a trasmitir teniendo en

cuenta las demás disposiciones del documento TI-G-01 Guía de intercambios de información .

- El almacenamiento, publicación, envío, edición, recepción, uso compartido, etc. de documentos o archivos que realice un usuario, debe cumplir con las leyes y normas vigentes sobre derechos de autor y propiedad intelectual vigentes en la República de Colombia y también con aquellas leyes y normas internacionales a las que el País se ha acogido bajo convenios internacionales, por lo tanto, el usuario no debe almacenar, publicar o compartir documento o archivos que infrinjan estas leyes y normas o convenios vigentes.

- El tratamiento y uso de datos personales que sean almacenados, suministrados, distribuidos o tengan algún tipo de tratamiento quedará supeditado y deberá dar cumplimiento a lo previsto en las directrices de ARN que se encuentran disponibles en: https://www.reincorporacion.gov.co/es/atencion/Paginas/politica-de-privacidad.aspx y contar con el concepto previo o autorización de la Oficina Asesora de Planeación.

- El usuario debe conectarse a través de Internet, teniendo en cuenta de disponer siempre de una conexión segura, estable, confiable y protegida con herramientas de seguridad como: Antivirus, Firewall, etc. Así mismo, el usuario es responsable de abrir y cerrar adecuadamente las sesiones de trabajo con el fin de evitar accesos no deseados y no autorizados.

- Las credenciales de conexión (nombre de usuario y contraseña) que le permiten al usuario de las herramientas de Microsoft 365 son de uso personal e intransferible a terceros. Por lo anterior, el usuario es el único responsable por toda la actividad y transacciones que se realicen dichas herramientas. La ARN no asumirá ninguna responsabilidad derivada de un uso inadecuado o ilegal de las credenciales del usuario.

- El usuario de la cuenta de OneDrive y el propietario del espacio de SharePoint Online debe periódicamente depurar la información mínimo cada seis (6) meses o cuando la cuota de almacenamiento este llegando al límite permitido, mediante la eliminación de información obsoleta y el traslado de la información definitiva al espacio destinado en carpetas compartidas.

- **Recomendaciones para el uso de las herramientas de OneDrive y SharePoint Online.**

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 5.1.3.8 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 y tenga las disposiciones de nombramiento de archivos según lo descrito en el documento GD- G-02 Guía para la administración y gestión de carpetas compartidas de archivo electrónico.
- ✓ 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, se deben guardar los archivos con las extensiones xlsx y docx.
- ✓ 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.

5.1.3.11 Política de intercambio de información

La ARN desarrolla acciones para 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 gestiona 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.

- **Normas de intercambio de información**

  - ✓ El Grupo de Gestión Contractual, 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, y/o solicitar los acompañamientos de otras dependencias cuando sea requerido. 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 propender 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 estos, 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 de 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.

5.1.3.12 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.

5.1.3.13 Política de trabajo en casa, teletrabajo o trabajo remoto

La ARN autorizará actividades de teletrabajo, trabajo en casa o trabajo remoto conforme a las condiciones del trabajo, los roles y perfiles de los empleados públicos. Las actividades de teletrabajo, trabajo en casa o trabajo remoto sólo se podrán llevar a cabo siempre y cuando se establezcan controles de seguridad alineados con las políticas de seguridad y privacidad de la información de la ARN y frente al respectivo análisis de riesgo.

La ARN dispondrá de los recursos tecnológicos y organizacionales para la adopción de un modelo de teletrabajo, trabajo en casa o trabajo remoto, que

permita cumplir con los intereses y necesidades de la entidad, considerando los riesgos y su respectiva gestión.

La ARN preverá mecanismos de seguridad física y lógica a los equipos y documentos requeridos para el desarrollo de las actividades de teletrabajo, con el fin de conservar las características de integridad, disponibilidad y confidencialidad de la información.

Antes de llevar a cabo cualquier actividad de teletrabajo, se definirán entre la Entidad y el empleado público, el alcance de las actividades a desarrollar y se determinarán como mínimo: la información a acceder, el horario de las actividades y los sistemas y servicios requeridos conforme la necesidad de la entidad y la legislación colombiana vigente.

En caso de pérdida o hurto de un equipo en el cual se lleven actividades de teletrabajo, trabajo en casa o trabajo remoto será responsabilidad del empleado público informar de forma inmediata a través del centro de servicios de la Entidad el evento, con el fin de establecer las medidas de seguridad adecuadas para la protección de la información contenida.

5.1.3.14 Política de gestión de comunicaciones y operaciones

La Oficina de Tecnologías de la Información es la encargada de: 1) la operación y administración de los recursos tecnológicos que soportan la gestión de la ARN ha definido las acciones para el manejo de los cambios a nivel de infraestructura, aplicativos, sistemas de información y servicios tecnológicos que son soportados por terceros y/o proveedores de acuerdo con lo descrito en el documento TI-G-09 Guía de gestión de cambios de tecnologías de la información. 2) 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.

- **Protección contra código malicioso**

La Oficina de Tecnologías de la Información debe contar con herramientas tales como antivirus, antimalware, antispam y antispyware que reduzcan el riesgo de contagio de software malicioso.

La Oficina de Tecnologías de la Información debe:

- ✓ Verificar que el software de antivirus, antimalware, antispyware y antispam cuente con las licencias de uso requeridas, certificando su autenticidad y la posibilidad de actualización periódica de las ultimas bases de datos de firmas del proveedor de servicios.
- ✓ Propender porque la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.
- ✓ Verificar que no se pueda realizar cambios en la configuración del software de antivirus, antispyware, antispam y antimalware por personal no autorizado.
- ✓ Propender que el software de antivirus, antispyware, antispam y antimalware posea las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.
- ✓ Realizar sensibilización a los empleados públicos y contratistas sobre la protección contra software malicioso y buenas prácticas de seguridad informática

Los empleados públicos, contratistas o terceros, deben abstenerse de abrir o ejecutar archivos y/o documentos de fuentes desconocidas, especialmente los que se encuentran en medios de almacenamiento externo o que provienen de correos electrónicos desconocidos.

Los empleados públicos, contratistas o terceros no deben descargar archivos de internet de fuentes desconocidas, en caso de requerirlo, debe generar la solicitud a la Oficina de Tecnologías de la Información a través del centro de servicios.

Los empleados públicos, contratistas o terceros que sospechen o detecten alguna infección por software malicioso deben notificar de inmediato a la Oficina de Tecnologías de la Información a través del centro de servicios, con el fin de ejercer los controles correspondientes.

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.

- **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 disco o cinta de la información y el resultado se registra a través de la herramienta de automatización de la tarea. La copia se realiza dependiendo del plan de backup correspondiente.
- ✓ **Backup Semanal**: Corresponde a la copia semanal completa en disco de la información y el resultado se registra a través de la herramienta de automatización de la tarea. La copia se realiza 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.

Las copias de seguridad de las bases de datos se generan y se resguardan en la herramienta de automatización de la tarea, de acuerdo con los planes diseñados.

La retención de las copias de seguridad varía dependiendo del tipo y programación el plan de generación de backup, dependiendo de la necesidad de cada uno de los servicios tecnológicos resguardados.

Los planes de copias de seguridad de la información y de restauración de copias de seguridad existentes pueden ser consultados en el gestor de conocimiento del Grupo de Infraestructura y soporte.

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 del Centro de Servicios a la extensión 10999 o al correo soporte@reincorporacion.gov.co.

- **Gestión de seguridad en redes**

La Oficina de Tecnologías de la Información debe:

- ✓ Proporcionar recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación del servicio de internet.
- ✓ Monitorear continuamente el tráfico del canal o canales que prestan el servicio de internet, con el fin de prevenir y atender cualquier incidente que se presente tan pronto como sea posible.
- ✓ Generar controles de navegación que eviten el ingreso a páginas, portales o servicios sospechosos o con código malicioso o catalogados como peligrosos, además se permitan accesos perfilados con base en las funciones u obligaciones contractuales de los usuarios.
- ✓ Proporcionar una infraestructura Tecnológica que soporte los sistemas de información y servicios internos. Esta debe estar segmentada a nivel de red física y lógica e independiente de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a internet. La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad.

- ✓ Establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.
- ✓ Mantener las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier otra tipificación que se considere conveniente para la Entidad.
- ✓ Instalar protección entre las redes internas y cualquier red externa, que este fuera de la capacidad de control y administración de la Entidad.
- ✓ Permitir el acceso a los servicios mediante plataformas de red inalámbricas protegidas con mecanismos de seguridad basados en autenticación de usuarios, perfiles de acceso, protocolos de conexión seguros y monitoreados.

- **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.

5.1.3.15 Política de seguridad en los procesos de desarrollo y de soporte

Lineamientos:

- La Oficina de Tecnologías de la Información debe propender por el desarrollo interno o externo de sistemas de información cumpla con las buenas prácticas para el desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado de acuerdo con lo descrito en el documento TI-G-06 Guía de desarrollo de software.
- La Oficina de Tecnologías de la Información debe establecer y mantener ambientes separados de Desarrollo/Pruebas y Producción.
- La Oficina de Tecnologías de la Información debe restringir el acceso a compiladores, editores y otros utilitarios del sistema operativo en el ambiente de producción, cuando no sean indispensables para el funcionamiento de este.
- La Oficina de Tecnologías de la Información debe asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con los últimos parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.

- La Oficina de Tecnologías de la Información ha definido las acciones para el manejo de los cambios en el software, aplicativos y sistemas de información de acuerdo con lo descrito en el documento TI-G-09 Guía de gestión de cambios de tecnologías de la información.
- Los desarrolladores internos y/o externos deben proporcionar un nivel adecuado de soporte para solucionar los problemas en los sistemas de información de la Entidad; de acuerdo con los niveles de servicio acordados entre las partes.
- Los desarrolladores internos y externos deben suministrar opciones de desconexión o cierre de sesión de los sistemas de información (Logout) que permitan terminar completamente con la sesión o conexión asociada.
- Los desarrolladores internos y externos deben remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.
- Los desarrolladores deben implementar controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en el repositorio destinado para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos solo tengan privilegios de lectura.
- Ni los desarrolladores ni terceros deben realizar pruebas, instalaciones o desarrollos de software, directamente sobre el entorno de producción. Esto puede conducir a fraude o inserción de código malicioso.
- Los desarrolladores deben asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.
- Todo desarrollo realizado por el equipo de la Oficina de Tecnologías de la Información o terceros debe estar alineado con los lineamientos de desarrollo seguro para Sistemas Información.

5.1.3.16 Política de control de acceso

El acceso a internet por parte de los empleados públicos y contratistas debe realizarse de acuerdo con el perfil de navegación definido por la Oficina de Tecnologías de la Información y asignado al usuario teniendo en cuenta las funciones u obligaciones contractuales según aplique el cual ha sido definido teniendo en cuenta las necesidades de los procesos de la Entidad.

La Entidad define 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.

- **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.

- **De los sistemas de información**

La Oficina de Tecnologías de la Información valida que los desarrollos internos y externos de los sistemas de información, cumplan con los requerimientos de seguridad adecuados para la protección de la información de la ARN para lo cual ha establecido una metodología que detalla los requerimientos de seguridad para el desarrollo, pruebas, puesta en producción y mantenimiento 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.

- **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.
  - ✓ Los empleados públicos y contratistas deben cerrar sesión en aplicaciones o sistemas de información al finalizar su uso dando clic en el botón de Salir o Cerrar sesión según corresponda.
  - ✓ 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 dependencia que delegue la Dirección General 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.

- **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.
- ✓ Formas de bloqueo:
- ✓ Tecla Windows + L;
- ✓ Teclas Ctrl+Alt+supr y seleccionar del menú la Opción bloquear.
- ✓ Estas opciones solo cierran el acceso al equipo y mantienen activas todas las aplicaciones que estén en curso.
- ✓ 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.

5.1.3.17 Política seguridad física y del entorno

La ARN debe adoptar medidas para la protección del perímetro de seguridad de sus instalaciones físicas para controlar el acceso y permanencia del personal en las oficinas, instalaciones y áreas restringidas (áreas destinadas al procesamiento o almacenamiento de información) con el fin de mitigar los riesgos y amenazas y evitar afectación a la confidencialidad, integridad y disponibilidad de la información.

Lineamientos:

- Las puertas y ventanas de las áreas seguras deben permanecer cerradas y bloqueadas cuando no haya supervisión o estén desocupadas.
- Todos los puntos de acceso deben tener un área de recepción con vigilancia u otro medio para controlar el acceso físico al sitio o instalación.
- Todos los empleados públicos, contratistas y visitantes que se encuentren en las instalaciones físicas de la ARN deben estar debidamente identificados con un carné que lo identifique y que debe portarse en lugar visible, asimismo debe portar el carné de la Administradora de Riesgos Laborales – ARL.
- Todo el personal que ingrese a las áreas seguras debe tener permiso del ingreso a la misma. Este debe estar acompañado por quien sea autorizado, éste se hará responsable de la estadía del personal ajeno a la ARN durante el tiempo que permanezca en las instalaciones.
- La Oficina de Tecnologías de la Información debe realizar mantenimientos preventivos a los centros de cableado que estén bajo su custodia; así mismo, se debe llevar el control al plan de mantenimiento de servicios tecnológicos.
- Las puertas de los centros de cableado deben permanecer cerradas.
- En el centro de datos y centros de cableado está prohibido: (fumar, ingresar comidas o bebidas, el porte de armas de fuego, corto punzantes o similares, mover, desconectar y/o conectar equipos sin autorización, modificar la configuración del equipo o interconectarlo sin autorización, alterar software instalado en los equipos sin autorización, alterar o dañar las etiquetas de identificación de los sistemas de información o sus conexiones físicas, extraer información de los equipos en dispositivos externos sin previa autorización)
- La Oficina de Tecnologías de la Información debe asegurar que los cables de potencia estén separados de los centros de comunicaciones siguiendo las normas técnicas pertinentes.
- La Oficina de Tecnologías de la Información debe controlar el acceso de visitantes a los centros de datos y centros de cableado que estén bajo su custodia.

5.1.3.18 Política de pantalla y escritorio limpio

- **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 etiquetada como información pública clasificada y/o información pública reservada que sea reproducida en equipos multifuncionales se debe retirar inmediatamente del equipo.

- **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 pública clasificada y/o información pública reservada 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.

5.1.3.19 Políticas de criptografía

- **Política de controles criptográficos**

La ARN protege 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.

- **Normas de controles criptográficos**

  - ✓ La herramienta de comunicación unificada usa las características de PKI en el sistema operativo Windows Server para proteger los datos clave que se usan para el cifrado de las conexiones de seguridad de la capa de transporte (TLS). Las claves utilizadas para el cifrado de medios se intercambian a través de conexiones TLS.
  - ✓ 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.

5.1.3.20 Política de relación con proveedores

- El Grupo de Gestión Contractual incluye en las minutas de los contratos y convenios clausulas y obligaciones en relación con la seguridad de la información y la protección de datos personales las cuales debe ser divulgadas a través de los supervisores de contratos a proveedores y terceros que debido al cumplimiento de las obligaciones contractuales cuando estos compartan, utilicen, recolecten, procesen, intercambien o consulten información.
- El Grupo de Gestión Contractual debe establecer en el momento de suscribirse contratos de cualquier tipo los riesgos asociados a la seguridad y privacidad de la información, los compromisos establecidos de confidencialidad de la información y el cumplimiento de las políticas de seguridad de la información de la ARN.
- El Grupo de Gestión Contractual debe establecer en los contratos con terceros y proveedores los requisitos legales y regulatorios relacionados con la protección de datos personales, los derechos de propiedad intelectual y derechos de autor.
- La Oficina de Tecnologías de la Información debe documentar, establecer controles y permisos cuando un tercero o proveedor requiera tener accesos a

la información por medio de la infraestructura tecnológica de la ARN de acuerdo con el formato TI-F-01 Solicitud de usuarios y/o recursos tecnológicos.

- Los supervisores de contratos deben verificar mensualmente el cumplimiento de Acuerdos de Nivel de Servicio establecidos.
- Los supervisores de contratos son los responsables de aplicar las políticas de seguridad de la información durante la ejecución de los contratos.
- La Oficina de Tecnologías de la Información ha definido las acciones para el manejo de los cambios a nivel de infraestructura, aplicativos y servicios tecnológicos que son soportados por terceros y/o proveedores de acuerdo con lo descrito en el documento TI-G-09 Guía de gestión de cambios de tecnologías de la información.

5.1.3.21 Política de gestión de incidentes de seguridad de la información

La ARN a través del Oficial de Seguridad de la Información promueve entre los empleados públicos y contratistas, el reporte y seguimiento de incidentes relacionados con la seguridad de la información.

5.1.3.22 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.

Los empleados públicos y contratistas deben informar al Centro de servicios cualquier evento anómalo o vulnerabilidad que detecten durante la operación de los equipos de cómputo, sistemas de información o aplicaciones.

- **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 estas.
  - ✓ 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.

5.1.3.23 Política de continuidad del negocio

De acuerdo con lo indicado en el documento GA-M- 06 Manual de continuidad del negocio a continuación se describe la política institucional establecida:

La Agencia para la Reincorporación y la Normalización -ARN, define herramientas que permiten una respuesta institucional efectiva y eficiente ante una emergencia o crisis, restableciendo en el menor tiempo posible sus funciones y la prestación de sus servicios. Para ello se basa en lo descrito en la familia de la norma ISO 27001, ISO 22301 y demás normativa legal relacionada con las temáticas de análisis y manejo de riesgos, seguridad digital, gestión de tecnologías de la información y gestión documental.

Para responder a situaciones de crisis que impacten la Continuidad del Negocio, la Entidad enmarcará sus acciones de acuerdo con la siguiente política:

- El Plan de Continuidad del Negocio está orientado a brindar los lineamientos para el restablecimiento oportuno de los procesos identificados como críticos, infraestructura y protección de los empleados públicos y contratistas, por la ocurrencia de eventos de interrupción o desastre, los cuales deben ser recuperados dentro de los márgenes de tiempo requeridos en el análisis de impacto para la continuidad del negocio.
- Los empleados públicos y contratistas de la ARN recibirán la formación y sensibilización para fortalecer las competencias e información respecto de las responsabilidades en el marco de la Continuidad del negocio.
- Los líderes de los procesos deben designar un Líder de Continuidad, quien es responsable de apoyar las actividades de la administración de continuidad de negocio para el proceso al que pertenece.
- El Plan de Continuidad del Negocio se debe revisar una (1) vez por año, sin embargo, se podrá revisar y actualizar antes, si así se requiere.
- Las actualizaciones en el Plan se priorizan según la criticidad de la fuente de cambio, algunas ameritarán cambios inmediatos, otras se añadirán a la revisión anual del Plan.
- El análisis de riesgos y del impacto en la Continuidad del Negocio debe realizarse una (1) vez por año, de acuerdo con lo definido en el DE-M-02 Manual de Gestión del Riesgo y en el numeral 6.3 del presente documento.
  •Las estrategias se revisarán cada vez que el Líder del Proceso lo considere o

como resultado del análisis de riesgos de acuerdo con la política de gestión de riesgos institucional en concordancia con lo establecido en el DE-M-02 Manual de Gestión del Riesgo.
- La Entidad debe contar con planes complementarios al de Continuidad del Negocio que deben revisarse una (1) vez por año o antes si así se requiere.

En este sentido la Agencia elabora y aprueba los siguientes instrumentos: Plan de Emergencias, Plan de Recuperación de Desastres (PRD) y Plan de Manejo de Crisis

Los resultados y el seguimiento de continuidad del negocio se presentan en el marco del Comité Institucional de Gestión y Desempeño.

- **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 no manipularlo o abrirlo, debe reportarlo inmediatamente al Centro de servicios a través de la extensión 10999, correo electrónico: soporte@reincorporacion.gov.co y.
- ✓ Evitar utilizar conexiones inalámbricas 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 al centro de servicios 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 con información institucional, guarde los documentos de la Entidad en los medios dispuestos por la ARN como **carpetas compartidas.**
- ✓ Si sospecha o detecta un incidente de seguridad de la información reportar al centro de servicios a través de los canales de comunicación establecidos.

5.2 DE LA PROTECCIÓN DE DATOS PERSONALES

5.2.1 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.

5.2.2 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 el software para la administración de la planeación y la gestión.

5.3 DE LOS DERECHOS DE AUTOR

La ARN propende 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.

5.3.1 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.

5.3.2 ASIGNACIÓN DE RESPONSABILIDADES

- Todos los empleados públicos o contratistas de la ARN deben dar cumplimiento de las 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 dependencia que delegue la Dirección General, apoyará el registro de los Derechos de Autor cuando corresponda.

5.3.3 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.

5.3.4 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 el portal 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.

6. LINEAMIENTOS DE OPERACIÓN MESA DE SEGURIDAD DE LA INFORMACIÓN

La Mesa de Seguridad de la información relaciona los aspectos de seguridad digital y seguridad de la información en su misionalidad que deben ser soportados por la gestión, políticas y procedimientos adecuados, que protejan los activos de información y la infraestructura que los contiene, en el marco de la normativa aplicable vigente.

6.1 ALCANCE MESA DE SEGURIDAD DE LA INFORMACIÓN

El alcance de la Mesa de Seguridad de la Información inicia con la identificación de los aspectos de seguridad digital y de seguridad de la información que requieren tratamiento, documentación, divulgación y presentación en las sesiones

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

de trabajo, continúa con la implementación y formalización de los aspectos de seguridad de la información a los cuales se les debe realizar seguimiento o escalamiento al Comité Institucional de Gestión y Desempeño y finaliza con la evaluación de mejora; aplica para todos los procesos de la ARN.

6.2 OPERACIÓN DE LA MESA DE SEGURIDAD DE LA INFORMACIÓN

El jefe de la Oficina de Tecnologías de la Información, como líder de la Política de Seguridad Digital, delega en el Oficial de Seguridad de la Información o Empleado Público o Contratista la gestión de la Mesa de Seguridad de la Información.

Por lo anterior, y teniendo en cuenta la temática en esta mesa de trabajo es necesario definir los lineamientos de operación de la Mesa de Seguridad de la Información, en el marco del cumplimiento de la normativa vigente y aplicable, que incluyen los aspectos de seguridad digital y seguridad de la información en su misionalidad que deben ser soportados por la gestión, políticas y procedimientos adecuados, que protejan los activos de información y la infraestructura que los contiene, que esté orientado a preservar los pilares fundamentales de Seguridad de la Información.

6.2.1 OBJETO DE LA MESA DE SEGURIDAD DE LA INFORMACIÓN

La Mesa de Seguridad de la Información dando cumplimiento a la política de Seguridad Digital emitida por MinTIC, tiene como objeto ser el órgano operativo y de apoyo para coordinar la incorporación de la seguridad de la información en los procesos, trámites, servicios, sistemas de información, infraestructura y en los activos de información identificados en la ARN, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

En cualquier caso, la Mesa de Seguridad de la Información no suplanta ninguna de las responsabilidades de seguridad de los empleados públicos y/o contratistas en sus funciones u obligaciones contractuales en este tema, en especial las del Oficial de Seguridad de la Información, el responsable de seguridad informática, el Asesor o Profesional Responsable de los temas de Seguridad en la Infraestructura Física, el Talento Humano y la Población Objeto.

6.2.2 INTEGRACIÓN

La Mesa de Seguridad de la Información está integrada así:

- El (La) Oficial de Seguridad de la Información como delegado del jefe de la Oficina de Tecnologías de la Información.
- El (La) jefe de la Oficina de Tecnologías de la Información
- El (La) responsable de Seguridad Informática- Profesional de la OTI
- El (La) subdirector(a) Técnico de Seguimiento de la Dirección Programática.
- El (La) subdirector(a) Técnico Territorial de la Dirección Programática.
- El (La) jefe de la Oficina Asesora de Planeación.
- El (La) jefe de la Oficina Asesora Jurídica.
- El (La) Asesor(a) de Talento Humano.
- Un delegado del Grupo de Gestión Documental.
- El (La) subdirector(a) Administrativo (a).
- El (La) Asesor(a) de seguridad y gestión del riesgo de la Dirección Programática.
- El (La) Asesor(a) del Grupo de Control Interno de Gestión, en calidad de invitado, con voz, pero sin voto.

NOTA 1: La citación a los integrantes se realizará de acuerdo con la temática a tratar en cada sesión. En estos casos, la representación en la Mesa de Seguridad de la información no puede ser delegada, por lo tanto, es deber de cada jefe o Asesor asistir. A la misma podrán asistir acompañantes con capacidad de apoyo para la toma de decisiones (las decisiones, están encaminadas a tener consenso de las temáticas que deben ser llevadas al Comité Institucional de Gestión y Desempeño).

NOTA 2: Si el tema no requiere de la presencia de un Directivo de acuerdo con la temática podrá delegar la participación.

6.2.3 FUNCIONES DE LA MESA DE SEGURIDAD DE LA INFORMACIÓN

- Establecer un acuerdo de trabajo anual en materia de seguridad de la información, al inicio de cada vigencia, con base en las revisiones realizadas al SGSI y la normatividad vigente aplicable.
- Aprobar las acciones emitidas, de acuerdo con las situaciones o eventos evidenciados por los integrantes de la Mesa de Seguridad de la Información, en cuanto el establecimiento de medidas o políticas relativas al tema de seguridad de la información, seguridad digital, ciberseguridad y ciberdefensa, cumplimiento normativo y protección de datos personales u otro que afecte la información sensible (incluye información reservada y clasificada) de la ARN.

- Realizar seguimiento a las novedades que puedan afectar el cumplimiento de los objetivos del SGSI y de la seguridad de la información sensible de la ARN ante incidentes de seguridad física y digital, de empleados públicos y contratistas, así como de las personas objeto de atención.
- A través del secretario de esta mesa, elevar los temas que puedan impactar los aspectos de seguridad de la información de la ARN, con el fin de ser puestos en conocimiento por parte del Comité Institucional de Gestión y Desempeño para la toma de decisiones en caso de que aplique.
- Realizar monitoreo bimensual al estado de implementación y seguimiento del Sistema de Gestión de Seguridad de la Información – SGSI.

6.2.4 SESIONES DE LA MESA DE SEGURIDAD

La Mesa de Seguridad de la Información se reunirá ordinariamente por lo menos una vez (1) cada mes, pero podrá reunirse extraordinariamente cada vez que sea necesario o en casos de requerirse atención urgente ante un incidente de seguridad de la Información u otro motivo de fuerza mayor. A dichas reuniones podrán asistir como invitadas las personas que se consideren necesarias de acuerdo con los asuntos a tratar.

6.2.5 MODALIDADES DE SESIÓN DE LA MESA DE SEGURIDAD

La mesa de seguridad tiene las siguientes modalidades de sesión:

- Presencial: las cuales se llevarán a cabo con la presencia de los integrantes en el lugar ordinario o extraordinario de sesiones de la mesa.
- Virtual: las cuales se llevarán a cabo a través de medios tecnológicos de interacción segura que se definan por la mesa.
- Mixtas: sesiones en las que podrá combinarse la modalidad presencial y virtual, según las circunstancias de orden administrativo, de salud, seguridad entre otras.

En ejercicio de su objeto y en atención a las problemáticas o necesidades de seguridad, la Mesa de Seguridad de la Información, sesiona en las instalaciones de la ARN tanto en la Sede Central como en los Grupos Territoriales, o en las instalaciones de entidades públicas o privadas.

6.2.6 QUORUM DE LAS SESIONES

La Mesa de Seguridad de la Información sesiona con la mitad más uno de sus integrantes. Si por falta de quórum no pudiere reunirse, se convocará a una segunda reunión que deberá efectuarse a más tardar en los cinco días siguientes,

contados desde la fecha fijada para la primera reunión. En la reunión de segunda convocatoria se conformará el quórum con la pluralidad de integrantes que se presenten.

6.2.7 VOTACIONES

Se entenderá por aprobado un tema para recomendar al Comité Institucional de Gestión y Desempeño o a la instancia que corresponda con la votación positiva de la mitad de sus miembros más uno.

6.2.8 SECRETARÍA TÉCNICA

La Secretaria Técnica está a cargo del Oficial de Seguridad de la Información o del empleado público o contratista delegado por el jefe de la Oficina de Tecnologías de la Información (responsable de la política de Seguridad Digital).

6.2.9 FUNCIONES DEL SECRETARIO(A) TÉCNICO

- Los borradores de actas son elaborados y enviados por la Secretaría Técnica a más tardar cinco días hábiles después de las reuniones. Si no se reciben observaciones, se dará por aprobado su contenido y será remitido a todos sus miembros la versión final.
- Elaborar el acta de reunión de la mesa y enviarlas, a la Oficina Asesora de Planeación una vez aprobadas y firmadas por los participantes, para custodia y en cumplimiento de la DE-G-10 Guía de operación para las mesas de trabajo del Comité Institucional de Gestión Desempeño.
- Llevar el archivo de las actas lo cual se realiza de acuerdo con las normas de archivo vigentes con base en lo estipulado en las tablas de retención documental y estarán en custodia del secretario técnico de la Mesa de Seguridad de la Información.
- Hacer seguimiento a los compromisos asumidos.
- Citar por instrucciones de alguno de los integrantes las sesiones de la Mesa de Seguridad de la Información.
- Apoyar al líder de política en el cumplimiento de los compromisos que resulten de las sesiones del Comité Institucional de Gestión y Desempeño.

NOTA: Los temas tratados dentro de la Mesa de Seguridad de la información se consideran confidenciales, por lo tanto, se solicita a los miembros de esta y aquellos que sean invitados a sus sesiones tratar esta información con sigilo y no hacerlos públicos.

6.2.10 RESPONSABILIDADES DEL OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

El Oficial de seguridad de la Información en lo que en materia de seguridad de la información se refiere, debe desarrollar las obligaciones contractuales y/o funciones descritas en este documento numeral "*5.1.2.2 Asignación de Responsabilidades – Coordinador de la Mesa de Seguridad de la Información"*.

La Mesa de Seguridad de la Información a través de su secretario técnico podrá solicitar información de contexto y estadísticas de seguridad a entidades públicas y/o privadas, así como a las diferentes dependencias, grupos internos de trabajo (GIT) y Grupos Territoriales (GT) de la ARN.

7. DOCUMENTOS DE REFERENCIA Y FUENTES DE INFORMACIÓN

- Manual de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.
- 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.