



AGENCIA PARA LA REINCORPORACIÓN Y LA NORMALIZACIÓN (ARN)

MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C. SEPTIEMBRE DE 2026

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

TABLA DE CONTENIDO

	Pág.
1. OBJETIVO.....	3
2. ALCANCE	3
3. DEFINICIONES	4
4. CONSIDERACIONES GENERALES	13
4.1 ASPECTOS TRANSVERSALES INSTITUCIONALES	13
4.2 CONTROLES DE LA DOCUMENTACIÓN DEL SGSI.....	13
4.3 REVISIÓN	14
4.4 ACCIONES POR INCUMPLIMIENTO DE LAS POLÍTICAS DEL SGSI	14
5. CONTENIDO Y DESARROLLO	14
5.1 DIRECTRICES DE LA SEGURIDAD DE LA INFORMACIÓN	14
5.2 OBJETIVOS Y POLITICA GENERAL DE SGSI	30
5.3 POLÍTICAS COMPLEMENTARIAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	31

 Agencia para la Reincorporación y la Normalización - ARN	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		CÓDIGO: TI-M-01
	FECHA 2026-09-08	VERSIÓN V- 14	

1 OBJETIVO

Establecer directrices y lineamientos para la protección de la seguridad de la información y Ciberseguridad, mediante la gestión segura de los activos dentro del Sistema de Gestión de Seguridad de la Información, con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de los datos e información, la capacidad de respuesta ante incidentes de seguridad y contribuir al cumplimiento de las metas estratégicas de la Agencia para la Reincorporación y la Normalización (ARN).

2 ALCANCE

El presente manual aplica a todos los procesos, áreas y niveles organizacionales de la Agencia para la Reincorporación y la Normalización (ARN). Las directrices y lineamientos aquí establecidos deben ser cumplidos por:

- **Funcionarios públicos** vinculados a la entidad.
- **Contratistas** que presten servicios bajo cualquier modalidad.
- **Terceros** que mantengan relaciones contractuales, comerciales o de colaboración con la ARN.

Su cumplimiento tiene como propósito establecer un nivel adecuado de protección de los activos de información y ciberseguridad sobre los activos de información, promoviendo la confidencialidad, integridad y disponibilidad de los datos, en concordancia con los principios de la seguridad de la información de la entidad.

Asimismo, se espera que todos los involucrados contribuyan activamente mediante la adopción de medidas preventivas y correctivas, orientadas al fortalecimiento del Sistema de Gestión de Seguridad de la Información (SGSI). Esta participación es esencial para el cumplimiento de las funciones institucionales, el respeto de las obligaciones legales y contractuales, y el logro de los objetivos estratégicos definidos en el presente manual.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

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 DE INFORMACIÓN: un activo de información se define como cualquier elemento —físico, digital, tangible o intangible— que tiene valor para la organización y que debe ser protegido para garantizar la seguridad de la información y ciberseguridad.

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.

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.

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

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

AUTORIZACIÓN: consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.

CIBERCRIMEN: se refiere a actividades delictivas que se llevan a cabo utilizando medios informáticos y digitales, como Internet o redes de comunicación. Esto puede incluir delitos como el robo de información personal, fraudes financieros, ataques de malware, y otros actos ilegales realizados mediante tecnología.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

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. Fuente MinTIC

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.

COLCERT: Grupo de Respuesta a Emergencias Cibernéticas de Colombia.

CONFIDENCIALIDAD: propiedad por la que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados. Fuente ISO:27000.

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).

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.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01
		FECHA 2026-09-08
		VERSIÓN V- 14

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

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

DISPONIBILIDAD: propiedad de ser accesible y utilizable bajo demanda por una entidad autorizada.

EAIS: corresponde al Equipo de Atención de Incidentes de Seguridad y se refiere al equipo especializado que se conforma para la atención del incidente de seguridad de la información. Este grupo está conformado por el equipo de seguridad informática y redes, el Oficial de Seguridad de la Información de la ARN y el centro de operaciones de seguridad (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.

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.

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

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

HERRAMIENTAS: son programas o aplicaciones que pueden ser utilizadas por muchas personas para apoyo 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 puede 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 puede divulgarse según las reglas establecidas en normas asociadas. (decreto 1081 de 2015: Artículo 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 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

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

(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: Artículo 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: propiedad de exactitud y completitud

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: la Mesa de Seguridad es la segunda instancia que se encuentra en el DE-M-11 Manual del Sistema Integrado de Gestión - SIG 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”.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

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.

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.

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.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		CÓDIGO: TI-M-01
			FECHA 2026-09-08 VERSIÓN V- 14

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.

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

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 (cibespacio), 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]: 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,

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

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 modalidad laboral que se efectúa en el marco de un contrato de trabajo o de una relación laboral dependiente, que consiste en el

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

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 o trabajadora en un sitio específico de trabajo.

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.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

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, planes, programas, 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 deben 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 para la gestión integral 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 del teletrabajo, AC-M-01 Manual para resolución de peticiones, quejas, reclamos, sugerencias y denuncias – PQRSD, 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 Personales, 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

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

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 los métodos de operación establecidos en el SIG para tal fin, GD-M-02 Manual para la producción de documentos, GD-P-04 Procedimiento control de documentos.

4.4 ACCIONES POR INCUMPLIMIENTO DE LAS POLÍTICAS DEL SGSI

Para los empleados públicos que estén involucrados en algún incumplimiento de la Política de Seguridad de la Información, la secretaria general adelanta las acciones necesarias teniendo en cuenta lo dispuesto en la Ley 1952 de 2019- Código General Disciplinario y en la Ley 2094 de 2021. Para los contratistas y terceros la secretaria general adelanta las acciones a las que haya lugar.

5 CONTENIDO Y DESARROLLO

5.1 DIRECTRICES 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 los 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.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

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 los datos e información 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 es la instancia encargada de orientar, articular y realizar seguimiento a la implementación y mejora continua del Modelo Integrado de Planeación y Gestión - MIPG en la entidad.

Con relación al Sistema de Gestión de Seguridad de la Información -SGSI- que aporta en las políticas de Gobierno Digital y Seguridad Digital; este comité aprueba la definición, orientación y seguimiento de las estrategias, lineamientos y acciones requeridas para su implementación, fortalecimiento y mejora continua, garantizando su alineación con los objetivos institucionales y la normativa vigente.

5.1.2.2 Mesa de Seguridad de la Información

Para el Sistema de Gestión de Seguridad de la Información -SGSI-, se ha conformado la Mesa de Seguridad de la Información como la instancia táctica y operativa, encargada de asesorar, coordinar, promover la gestión de los diferentes aspectos relacionados con la seguridad de la información en la entidad y/o presentar propuestas decisoras al Comité Institucional de Gestión y Desempeño.

Esta mesa tiene como propósito articular acciones orientadas a la protección de la seguridad en la información en la entidad relacionadas con la infraestructura tecnológica y física, así como los recursos humanos involucrados en los procesos que contribuyen a la protección de la confidencialidad, integridad y disponibilidad de la información.

Asimismo, constituye una instancia interdisciplinaria que facilita la formulación, implementación y seguimiento de acciones en el marco del SGSI y de las políticas de Gobierno Digital y Seguridad Digital, contando para ello con el respaldo y apoyo de la Alta Dirección.

En el presente documento se describen la conformación de la Mesa de Seguridad de la Información, las responsabilidades de sus integrantes y los lineamientos establecidos para su funcionamiento y operación.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

5.1.2.3 Asignación de responsabilidades

El Comité Institucional de Gestión y Desempeño:

Las responsabilidades se abordan en el DE-M-11 Manual del Sistema Integrado de Gestión – SIG-, en lo relacionado con “Responsabilidades en el sistema integrado de gestión”.

La mesa de seguridad de la información está encargada de la articulación, coordinación, análisis y estudio de las siguientes temáticas:

- Seguridad en la infraestructura tecnológica de la ARN
- Sistema de Gestión de Seguridad de la Información
- Ciberseguridad en la ARN

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 cuenta con los 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, identificación de riesgos, asesoría en aplicación de metodología adoptadas por la entidad en la 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 de información de criticidad alta, y monitoreando cambios significativos sobre los mismos.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

- Participar 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 planes, programas, 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 al plan de continuidad de negocio de la entidad liderado por la subdirección administrativa, y actividades asociadas al proyecto DATA LOSS PREVENTION – DLP de la ARN, con el propósito de evitar la fuga de información.
- Acompañar la implementación de 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 políticas de seguridad informática y de 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 en temas, requerimientos y demás comunicaciones internas y externas de seguridad de la información.
- Ejercer la secretaría técnica de la mesa de seguridad de la información, documentando su gestión mediante actas o informes o documentos de seguimiento o complementarios.

Responsable de seguridad informática:

El (la) 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 y ciberseguridad.

La ARN brinda recursos para que el responsable de seguridad Informática pueda desarrollar las actividades a su cargo:

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

- Elaborar, documentar, actualizar, monitorear y hacer seguimiento al Plan del Sistema de Gestión de Seguridad de la Información y gestión de riesgos que incluye la revisión y evaluación 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 de la información y gestión de riesgos de la Información, que incluye. monitorear la ocurrencia de violaciones de seguridad y aplicar acciones correctivas.
- Liderar y articular la planeación, ejecución, administración, gestión, monitoreo, evaluación y 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 de la Información.
- Participar, con previa comunicación, 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 en temas de seguridad informática.
- Participar en pruebas de planes de contingencia que aseguren la disponibilidad de los servicios tecnológicos y sistemas de información de la Entidad, que se encuentren a cargo de la Oficina de tecnologías de la información para evaluar la fortaleza de la seguridad y detectar 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

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

confidencialidad en el sistema de información y demás aplicativos misionales y de apoyo de la Entidad.

5.1.2.4 Roles y responsabilidades en los sistemas de información, aplicativos, sede electrónica y/o servicios de tecnologías de la información

Oficina de Tecnologías de la Información

La Oficina de Tecnologías de la Información implementa y gestiona las plataformas y herramientas para el monitoreo y control de la seguridad de la información de la entidad.

La Oficina de Tecnologías de la Información procura 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, promueve la adecuada gestión de la seguridad de la información de la entidad.

Personal Directivo de la Agencia para la Reincorporación y la Normalización

El (la) director(a) General, el (la) Secretario(a) General, el(la) Director(a) Programático (a), el (la) Jefe Oficina Asesora de Planeación, el(la) Jefe Oficina Asesora Jurídica, el(la) Jefe Oficina Asesora de Comunicaciones, el(la) Jefe Oficina de Tecnologías de la Información y los (las) 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(las) empleados(as) 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.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

Todo(as) los (las) empleados(as) 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 compromiso y autorización sobre confidencialidad y manejo de la información.

Propietario de los activos de información

Es el(la) empleado(a) 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.
- Asegurar la confidencialidad, integridad y disponibilidad de los activos de información a su cargo.
- Sensibilizar sobre los controles de los activos de información del cual es propietario a los custodios y usuarios de estos.
- Efectuar una verificación de los controles requeridos sobre los activos de información bajo su responsabilidad.

Custodio de los activos de información

Es el(la) empleado(a) o contratista o dependencia de la Entidad responsable de la protección, seguridad, accesibilidad y mantenimiento adecuado de los activos de información bajo su cuidado. Sus principales responsabilidades son:

- Aplicar las políticas de seguridad de la información
- Gestionar el acceso a los activos de información
- Implementar y mantener los controles requeridos en los lugares donde estén almacenados los activos de información que se encuentren a su cargo.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

- Proteger los activos de información a su cargo frente al almacenamiento, transporte y procesamiento.

Líder de procesos

Es el(la) empleado(a) público o dependencia de la Entidad que lidera y tiene 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(l)(los) propietario(s) de los activos de información de su proceso.
- Gestionar los riesgos de seguridad de la información asociados a los activos de información identificados en el proceso, teniendo en cuenta el manual de gestión del riesgo.
- Atender y apropiar los lineamientos y políticas de seguridad de la información dentro del proceso liderado.

Personal con perfil de usuario

Todos los usuarios de la Entidad 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, integridad y disponibilidad 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 continuar aplicando la confidencialidad de la información.
- Conocer y cumplir el Manual del Sistema de Gestión de Seguridad de la Información emitido por la entidad, procedimientos e instructivos internos, relacionados con la 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 emitidos por Grupo de Gestión Contractual.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

- Usar de forma adecuada los Sistemas de información con sus respectivos procedimientos, mecanismos y controles de acceso.
- Utilizar las contraseñas de forma adecuada, no compartirlas, ni exponerlas, ya que son de carácter personal y de uso exclusivo.
- Los empleados públicos o contratistas que tengan sospechas de que su acceso autorizado ha sido vulnerado o está siendo utilizado por otra persona, deben realizar el cambio de inmediato de la contraseña y comunicar éste u otros incidentes de seguridad de la información al Centro de Servicios, a la extensión 10999 o al correo Centro de Servicios ARN (Centro de Servicios ARN (soporte@reincorporacion.gov.co)).

Personal con acceso privilegiado

Los (las) empleados (as) públicos o contratista(s) con acceso privilegiado, deben cumplir con las mismas responsabilidades del personal con perfil de usuario, teniendo mayor reserva al acceder, realizar cambios o ajustes a la infraestructura tecnológica, datos 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 los sistemas de información adoptados por la Agencia para la Reincorporación y la Normalización.
- Salvaguardar la información almacenada en los sistemas de información que tengan bajo su responsabilidad.
- Gestionar los accesos de 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 cualquier evento o incidente 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 en materia de seguridad de los sistemas de información de la Agencia para la Reincorporación y la Normalización.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

Líder o administrador funcional:

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

Las responsabilidades específicas del 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 estén acordes a los procesos de la Entidad.
- Liderar el análisis desde el punto de vista funcional, del sistema de información, aplicación o infraestructura de TI que lidera y establecer las necesidades y requerimientos.
- Administrar los usuarios 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 del sistema de información, aplicación o infraestructura de TI bajo su responsabilidad.
- Participar en la elaboración y divulgación del plan de contingencia que debe ejecutarse cuando el sistema de información, aplicación o infraestructura de TI no se encuentre disponible para garantizar la continuidad en el proceso funcional.
- Informar al centro de servicios los incidentes que detecte en la información del sistema de información o 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 del sistema de información, aplicación o infraestructura de TI cuando sea requerido, implementando acciones necesarias para la mejora.

Líder técnico:

"Toda impresión física de este documento se considera Documento no Controlado.
La versión vigente se encuentra en el software para la administración de la planeación y la gestión"

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

Corresponde a un empleado(a) público o contratista quien es el 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.
- Promover por 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 disponible 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(la) encargado(a) de gestionar los servicios a su cargo desde el punto de vista tecnológico (planeación, diseño, operación, mantenimiento, monitoreo y acciones de mejora).

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		CÓDIGO: TI-M-01
			FECHA 2026-09-08 VERSIÓN V- 14

Administrador de bases de datos de la ARN: es el(la) empleado(a) público encargado de la gestión de las bases de datos de la ARN.

Personal del centro de servicios: 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: está encargada de la seguridad informática de la ARN.

5.1.2.5 De las autoridades frente al SGSI

Las modificaciones que impactan la política general del SGSI, son aprobadas 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: Oficial de Seguridad de la Información
- Segunda Instancia: Mesa de Seguridad de la Información

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

- Tercera instancia: 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 Lineamientos de operación mesa de seguridad de la información

La Mesa de Seguridad de la información monitorea 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.

5.1.3.1 Alcance mesa de seguridad de la información

El alcance de la Mesa de Seguridad de la Información inicia con la identificación, evaluación y las aprobación pertinente de los aspectos de seguridad digital y de seguridad de la información que requieren tratamiento, documentación, divulgación y presentación en las sesiones 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; aplica la divulgación para todos los procesos de la ARN.

5.1.3.2 Operación de la mesa de seguridad de la información

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

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		CÓDIGO: TI-M-01
		FECHA 2026-09-08	VERSIÓN V- 14

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.

5.1.3.3 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(las) empleados(as) públicos y/o contratistas en sus funciones u obligaciones contractuales en este tema, en especial las del Oficial de Seguridad de la Información, el(la) responsable de seguridad informática, el(la) Asesor(a) o Profesional Responsable de los temas de Seguridad en la Infraestructura Física, el Talento Humano y la Población Objeto.

5.1.3.4 Integrantes de la mesa de seguridad de la información

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.
- El (La) Coordinador(a) del Grupo de Gestión Documental.
- El (La) subdirector(a) Administrativo (a).
- El (La) Asesor(a) de seguridad y gestión del riesgo de la Dirección General.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

- El (La) Asesor(a) del Grupo de Control Interno de Gestión, en calidad de invitado, con voz, pero sin voto.

NOTA 1: la convocatoria a los integrantes de la Mesa de Seguridad de la Información se realiza a los titulares designados. No obstante, los miembros pueden delegar su participación cuando existan circunstancias que les impidan asistir. En estos casos, el delegado puede intervenir en las deliberaciones, presentar los insumos técnicos requeridos y apoyar el análisis de los temas tratados; sin embargo, la facultad de emitir voto y adoptar decisiones sobre los asuntos sometidos a consideración es exclusiva del titular del cargo, por lo que no puede ser ejercida por el delegado.

5.1.3.5 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(as) 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 trimestral al estado de implementación y seguimiento del Sistema de Gestión de Seguridad de la Información – SGSI.

5.1.3.6 Sesiones de la mesa de seguridad

La Mesa de Seguridad de la Información se reúne ordinariamente por lo menos una vez (1) cada mes, pero puede 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

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

pueden asistir como invitadas las personas que se consideren necesarias de acuerdo con los asuntos a tratar.

5.1.3.7 Modalidades de sesión de la mesa de seguridad

La mesa de seguridad tiene las siguientes modalidades de sesión:

- Presencial: las cuales se llevan a cabo con la presencia de los integrantes en el lugar ordinario o extraordinario de sesiones de la mesa.
- Virtual: las cuales se llevan a cabo a través de medios tecnológicos de interacción segura que se definan por la mesa.
- Mixtas: sesiones en las que puede 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.

5.1.3.8 Quorum de las sesiones

La Mesa de Seguridad de la Información sesiona con la mitad más uno de sus integrantes y/o delegados. Si por falta de quórum no pueden reunirse, se convoca a una segunda reunión que debe 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 conforma el quórum con la pluralidad de integrantes que se presenten.

5.1.3.9 Votaciones

Se entiende 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.

5.1.3.10 Secretaría técnica

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

5.1.3.11 Funciones del secretario(a) técnico

"Toda impresión física de este documento se considera Documento no Controlado.
La versión vigente se encuentra en el software para la administración de la planeación y la gestión"

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

- 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 da por aprobado su contenido y se remite 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 operativa para las mesas de trabajo de las políticas de gestión y desempeño institucional del MIPG.
- 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 están bajo la 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.

5.1.3.12 Responsabilidades del(la) oficial de seguridad de la información

El(la) 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 “*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 pueden 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.

5.2 OBJETIVOS Y POLITICA GENERAL DE SGSI

Los objetivos y la política general del del Sistema de Gestión De Seguridad De La Información (SGSI), se encuentran dentro del DE-M-11 Manual Del Sistema Integrado De Gestión.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

5.3 POLÍTICAS COMPLEMENTARIAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

5.3.1 Política Ciberdefensa y ciberseguridad en la ARN

- En la ARN se da cumplimiento a la protección de la seguridad digital, en todo lo referente con la Ciberdefensa y Ciberseguridad del Estado Colombiano en coordinación con los entes responsables de esta labor.
- Cualquier evento materializado relacionado con ataque cibernético tales como cibercrimen, ciber lavado, ciber espionaje, ciberterrorismo, entre otros, es atendido por la ARN de acuerdo con los protocolos establecidos por los entes nacionales encargados, siendo la comunicación hacia estos teniendo en cuenta la TI-G-04 guía para la gestión de incidentes de seguridad.
- La Oficina de Tecnologías de la Información debe realizar concienciación a los empleados públicos y contratistas en buenas prácticas de ciberseguridad.
- La Oficina de Tecnologías de la Información debe realizar pruebas de Ethical Hacking y escaneos de vulnerabilidades de acuerdo con lo establecido en el TI- G-10 Guía de gestión de vulnerabilidades, con el fin de detectar debilidades antes que puedan ser explotadas.
- Toda actividad de pruebas, monitoreo o gestión de incidentes que implique tratamiento de datos personales debe garantizar su anonimización, minimización y tratamiento conforme al DE-M-06 Manual de Protección de Datos Personales.

5.3.2 Gestión del riesgo de seguridad digital

La Agencia para la Reincorporación y la Normalización establece la presente Política de Gestión del Riesgo y Seguridad Digital como parte integral del Sistema de Gestión de Seguridad de la Información (SGSI), con el propósito de proteger la confidencialidad, integridad y disponibilidad de la información en concordancia debe promover el uso responsable del entorno digital por parte de funcionarios públicos y contratistas, acatando para ello las directrices establecidas en los CONPES 3854 de 2016 y CONPES 3995 de 2020. con los requisitos de la Norma ISO/IEC 27001:2022, la Política Nacional de Seguridad Digital y los lineamientos definidos en los documentos CONPES 3854 de 2016 y 3995 de 2020.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

La ARN debe adoptar un enfoque sistemático, basado en riesgos, para la identificación, análisis, evaluación, tratamiento, aceptación, y monitoreo de los riesgos de seguridad digital y riesgos cibernéticos, que puedan afectar sus procesos, servicios, activos de información, infraestructura tecnológica y el cumplimiento de su objeto misional, fortaleciendo la continuidad de la operación y la confianza de las partes interesadas.

La gestión de riesgos de seguridad digital debe orientarse a prevenir situaciones o ataques que puedan afectar la seguridad de la información de la ARN, incluyendo, de manera enunciativa, gusanos, ingeniería social, keyloggers, phishing, ransomware, spamming, sniffers, spoofing y troyanos. La ejecución y supervisión de esta labor está a cargo del Oficial de Seguridad Informática. Los funcionarios y contratistas deben reportar y con carácter obligatorio, los riesgos de seguridad digital y de la información identificados por medio de la herramienta de gestión como un evento de seguridad.

5.3.3 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

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

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(a) 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.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

5.3.4 Política de gestión de activos

La Agencia para la Reincorporación y la Normalización establece la presente Política de Gestión de Activos como parte integral de su Sistema de Gestión de Seguridad de la Información (SGSI), con el fin de garantizar la protección adecuada de los activos de información durante todo su ciclo de vida, asegurando su confidencialidad, integridad y disponibilidad.

- La ARN protege los activos de información que utilice sean de su propiedad, arrendados o suministrados por terceros, los cuales deben emplearse exclusivamente para el desarrollo de las funciones laborales o el cumplimiento de las obligaciones contractuales, de conformidad con la normativa vigente y las políticas institucionales.
- La ARN debe proporcionar a los(las) empleados(as) públicos y contratistas de acuerdo con las necesidades institucionales, los equipos de cómputo, dispositivos y programas informáticos autorizados para el desempeño de sus funciones. La Oficina de Tecnologías de la Información implementa controles técnicos de seguridad, incluyendo la restricción del uso de puertos USB u otros medios extraíbles en los equipos de cómputo propiedad de la entidad. Cualquier habilitación temporal debe ser solicitada a través del Centro de Servicios, diligenciando la TI-F-01 Solicitud de usuarios y/o recursos tecnológicos, conforme a los procedimientos establecidos.
- La asignación, uso y gestión de los activos de información para terceros proveedores o contratistas se realiza en coordinación con las dependencias responsables y los supervisores de los contratos, garantizando que dichos activos cuenten con las medidas de seguridad, licenciamiento y controles definidos por la ARN.
- La ARN es titular de los derechos propiedad intelectual de los desarrollos tecnológicos e intelectuales generados por los(las) empleados(as) públicos y contratistas en desarrollo de sus funciones en cumplimiento del objeto del contractual, de acuerdo con la legislación vigente y las cláusulas contractuales suscritas.
- La ARN es propietaria de los activos de información y los administradores. Los propietarios de los activos son los líderes de proceso o responsables designados, y los administradores de los activos son los empleados públicos o contratistas autorizados, responsables de la adecuada gestión, protección y uso de la información, sistemas de información, aplicaciones, hardware,

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

infraestructura tecnológica y activos físicos tales como documentos y bases de datos manuales.

- Los(las) empleados(as) públicos y contratistas deben garantizar que la información de la ARN contenida en los equipos asignados no se pierda, altere o divulgue sin autorización. En el caso de información clasificada o reservada, cualquier copia, traslado o reproducción debe contar con autorización previa del jefe inmediato o del supervisor del contrato, según corresponda, de conformidad con la clasificación de la información establecida por la entidad. La copia, sustracción, daño intencional o uso indebido de la información es sancionado conforme a la normativa vigente.
- Todos los empleados públicos y contratistas deben cumplir las disposiciones relacionadas con la protección de datos personales, derechos de autor, transparencia y acceso a la información pública, así como las normas definidas en el Manual del Sistema de Gestión de Seguridad de la Información de la ARN.
- La gestión, baja y disposición final de los activos tecnológicos debe cumplir el Programa de Gestión Integral de Residuos de Aparatos Eléctricos y Electrónicos (RAEE) y lo establecido en el documento GA-M-02 Manual para el manejo y control administrativo de los bienes de la entidad, bajo la responsabilidad del Grupo de Almacén e Inventarios.
- En los casos de contratistas ocasionales o convenios con otras entidades, las dependencias responsables deben definir los equipos y software necesarios para el cumplimiento de las obligaciones contractuales, los cuales deben contar con licenciamiento válido, actualizaciones vigentes y software antivirus autorizado. El uso de dichos equipos debe ser informado a la Oficina de Tecnologías de la Información. Está prohibido el uso de software no autorizado por la OTI.
- La Oficina de Tecnologías de la Información realiza revisiones periódicas del Hardware, Software y herramientas informáticas utilizados en cada dependencia de la ARN. La descarga, instalación o uso de aplicativos no autorizados constituye una violación a las Políticas de Seguridad de la Información y es reportada al Oficial de Seguridad de la Información para la adopción de las medidas correspondientes.
- Cuando sea necesario y previa autorización de la Mesa de Seguridad de la Información, el personal autorizado de la Oficina de Tecnologías de la Información puede acceder a revisar los activos de información creados,

"Toda impresión física de este documento se considera Documento no Controlado.

La versión vigente se encuentra en el software para la administración de la planeación y la gestión"

Página 35 de

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		CÓDIGO: TI-M-01
		FECHA 2026-09-08	VERSIÓN V- 14

almacenados, enviados o recibidos por los usuarios en los equipos informáticos asignados, con el fin de garantizar el cumplimiento de las políticas de seguridad de la información. Los recursos informáticos de la ARN no pueden ser utilizados para fines personales, comerciales, publicitarios, políticos, religiosos o cualquier otro uso no autorizado.

- Los activos de información de la ARN deben ser identificados, clasificados y controlados, de manera que se garantice su uso adecuado, protección y recuperación ante desastres, conforme a lo establecido en el DE-I-03 Instructivo para la actualización de la matriz de activos de información
- El Grupo de Almacén e Inventarios es responsable de llevar y administrar el inventario valorizado de hardware y software de propiedad de la ARN, así como el control de los equipos arrendados, discriminado por dependencias y de acuerdo con lo establecido en el documento GA-M-02 Manual para el Manejo y Control Administrativo de Bienes de la Entidad.
- Los usuarios no deben realizar actos que impliquen el uso inadecuado de los recursos tecnológicos, tales como el envío de correos electrónicos masivos con fines no institucionales o la utilización de aplicaciones y juegos en línea no autorizados.
- El Grupo de Gestión Documental, mediante la implementación de instrumentos archivísticos como la Tabla de Retención Documental, el Programa de Gestión 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.
- Los usuarios no pueden, sin autorización previa de la Oficina de Tecnologías de la Información:
 - Instalar, descargar o copiar software en los equipos de la ARN.
 - Modificar, transformar, adaptar, descompilar o realizar ingeniería inversa sobre software propiedad de la ARN.
 - Distribuir software institucional por cualquier medio.

Inventario de activos de información

La ARN realiza la actualización del inventario de activos de información mínimo una vez al año, bajo la responsabilidad de cada propietario y con el liderazgo de la

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

Oficina de Tecnologías de la Información. Este inventario debe reflejar el estado, clasificación, responsables y controles asociados a cada activo.

5.3.5 Clasificación de la información

Los líderes de los procesos deben cumplir con los mecanismos y procedimientos establecidos en la entidad para la adecuada clasificación, calificación, manejo y tratamiento de los activos de información, de acuerdo con el GD-I-08 Instructivo de Clasificación y etiquetado de la información. Dependiendo del nivel de confidencialidad, integridad y disponibilidad que se requiera para su protección.

Los líderes de procesos deben validar las restricciones y niveles de acceso establecidos para los activos de información categorizados como públicos clasificados y públicos reservados.

5.3.6 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 promover que se cumplan los principios de seguridad de la información relacionados con la confidencialidad, integridad y disponibilidad, la entidad pone a disposición los recursos de almacenamiento los cuales son: carpetas compartidas, OneDrive® y SharePoint Online de Microsoft 365®.

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

Los nombres de 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.

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.

De las carpetas compartidas

La ARN debe poner a disposición de los(las) empleados(as) públicos y contratistas el acceso a las carpetas compartidas a través de conexiones seguras por VPN / Escritorio Remoto o directamente en los dispositivos asignados por la entidad.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

Carpetas compartidas de apoyo

Las carpetas compartidas sobre la infraestructura ofrecida por la OTI son 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, debe asignar 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 la TI-F-01 Solicitud de Usuario y/o Recursos Tecnológicos dispuesto en SAPYG.

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

Cada administrador de las carpetas compartidas debe 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.

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, los cuales deben dar cumplimiento a lo establecido en el TI-M-02 Plan de Preservación Digital a Largo Plazo, la GD-G-02 Guía para la Administración y Gestión de Carpetas Compartidas de Archivos Electrónicos, y con las Tablas de Retención Documental vigentes.

El acceso y administración de esta estructura de carpetas compartidas se encuentran a cargo del responsable con apoyo del grupo 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

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

inmediato y/o coordinador y finaliza con la consolidación y tramite de estas solicitudes por parte del Grupo de Gestión Documental, a través de un caso registrado al centro de servicios tecnológicos.

Almacenamiento en nube de información

Los recursos de almacenamiento como, OneDrive® y SharePoint Online de Microsoft 365®, aprovisionados por la ARN para los usuarios, deben estar exentos de publicaciones de archivos de tipo ejecutable, si la dependencia requiere hacer uso de algún ejecutable debe informar de la necesidad 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.

De OneDrive® y SharePoint Online de Microsoft 365®

Los recursos de almacenamiento provistos por la ARN para los usuarios con dominio @reincorporación.gov.co, deben utilizarse exclusivamente para archivos relacionados con funciones laborales o contractuales, por lo anterior se debe abstener de alojar archivos personales, música, videos, imágenes u otros no vinculados al trabajo.

Cada usuario o área, según corresponda, debe ser el responsable de administrar y mantener actualizados los accesos a la información alojada en los servicios de almacenamiento, como OneDrive y SharePoint Online. Esto incluye la gestión de miembros, propietarios y permisos en los Grupos de Microsoft 365, así como en los sitios y recursos asociados, garantizando el control y conocimiento sobre quiénes tienen acceso a los recursos compartidos y, por ende, a la información allí alojada.

El usuario de OneDrive y el propietario del sitio en SharePoint Online debe monitorear las alertas emitidas por los servicios, depurar la información periódicamente (al menos cada seis meses o cuando la cuota de almacenamiento esté próxima al límite), y antes de liberar espacio verificar el contenido para evitar duplicidad o eliminar información innecesaria y trasladar la documentación definitiva a los sitios de SharePoint Online asociados a los Grupos de Microsoft 365, siguiendo las indicaciones del jefe inmediato o supervisor. En caso de requerir ampliación de espacio, se debe registrar la solicitud en la herramienta de gestión.

Gestión y disposición de medios removibles

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

Todos los dispositivos y unidades de almacenamiento de la entidad que sean removibles, tales como, Cd, DVDs, dispositivos “USB”, discos duros externos, cámaras fotográficas, cámaras de video (No de vigilancia), entre otros, que se conecten a la red de datos de la ARN o que se encuentren bajo su custodia, debe estar sujetos mediante la gestión de las herramientas tecnológicas de control de la ARN.

El responsable del dispositivo debe verificar 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.

Borrado seguro de información

Todos los medios de almacenamiento que contengan información de la ARN, que sean reasignados y aquellos equipos que contengan medios de almacenamiento que vayan a ser dados de baja deben seguir los procedimientos de borrado seguro ejecutados por la OTI, lo cual busca que la información no sea recuperable (Aplica para medios de almacenamiento, equipos de cómputo, discos duros externos, etc.).

Transferencia de información en medios físicos

Toda transferencia de medios físicos debe cumplir con las disposiciones de seguridad indicadas en el documento TI-G-01 Guía de Intercambio de Información.

5.3.7 Política de uso de OneDrive® y SharePoint Online de Microsoft 365®

- En los espacios colaborativos de Microsoft 365 (como grupos o sitios de SharePoint Online), los propietarios son responsables de determinar si los miembros pueden compartir información y conceder accesos, conforme a las necesidades institucionales y las políticas vigentes. El uso está permitido únicamente a empleados públicos y contratistas activos de la ARN que cuenten con una cuenta institucional vigente del dominio @reincorporacion.gov.co. El propietario es responsable de administrar los permisos específicos, gestionar el espacio, asignar miembros y garantizar el acceso adecuado a la información y documentación almacenada.
- El usuario debe depurar la información almacenada en OneDrive y, antes de ausentarse por vacaciones, descanso, finalización de contrato o renuncia, debe trasladar los archivos a los sitios de SharePoint Online asociados a sus Grupos de Microsoft 365, siguiendo las indicaciones del supervisor o jefe inmediato. Asimismo, los miembros e invitados de los grupos de Microsoft 365 con

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

espacios en SharePoint Online son responsables de la gestión de la información allí almacenada, conforme a los permisos y roles asignados por el propietario.

- 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 queda supeditado y debe 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.
- 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 seguir lo indicado en el documento GD-I-08 Instructivo de Clasificación y Etiquetado de Información, así mismo deben previamente establecer un convenio, cifrar la información a transmitir teniendo en cuenta las demás disposiciones del documento TI-G-01 Guía de Intercambios de información.
- El usuario debe conectarse a través de Internet, teniendo en cuenta que debe disponer siempre de una conexión segura, estable, confiable y protegida con herramientas de seguridad. Así mismo, el usuario debe ser responsable de abrir y cerrar adecuadamente las sesiones de trabajo de las cuentas asignadas de la Entidad 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 el uso de las herramientas de Microsoft 365 son personales e intransferible. Por lo anterior, el usuario es el único responsable por toda la

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

actividad y transacciones que se realicen dichas herramientas. La ARN no asumirá ninguna responsabilidad derivada de un uso inadecuado o ilegal.

5.3.8 Política de intercambio de información

Desarrolla acciones de protección de la información en todos los escenarios de intercambio, independientemente del medio, formato o tecnología utilizada, conforme a la normativa aplicable a la entidad y a los lineamientos definidos en la TI-G-01 Guía de Intercambio de Información, la cual constituye el marco operativo para la implementación de esta política.

Todo intercambio de información con terceros debe formalizarse mediante contratos, convenios o instrumentos jurídicos que incluyan Acuerdos de Confidencialidad y/o Acuerdos de Intercambio de Información, en los que se establezcan de manera expresa las responsabilidades, obligaciones, limitaciones de uso, medidas de protección, condiciones de eliminación de la información y las consecuencias legales derivadas de su divulgación, uso indebido o incumplimiento. La ARN garantiza que el intercambio de información se realice utilizando tecnologías informáticas seguras, medios de transmisión confiables y controles técnicos y organizacionales adecuados, de acuerdo con el nivel de clasificación de la información, el análisis de riesgos de seguridad de la información y los requisitos legales aplicables. Para el intercambio de información en medio físico se establecerán directrices específicas que aseguren su custodia, transporte y trazabilidad.

Cuando el intercambio de información lo requiera, se debe implementar mecanismos de cifrado, anonimización o seudonimización, especialmente para información clasificada, reservada, datos personales, datos sensibles o información privada, con el fin de prevenir accesos no autorizados, pérdida, alteración o divulgación durante la transferencia.

El intercambio de información debe regirse por el principio de mínima información necesaria, garantizando que únicamente se compartan los datos estrictamente requeridos para el cumplimiento del objeto del intercambio, previo consentimiento de los titulares cuando aplique, salvo en los casos expresamente autorizados por la ley o por requerimientos de autoridades competentes o entes de control.

Todos los intercambios de información deben contar con mecanismos de trazabilidad que permitan identificar el origen, destino, fecha, responsables y condiciones del intercambio, así como facilitar el seguimiento, control y auditoría de dichas transacciones.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

Lineamientos para el intercambio de información:

- El Grupo de Gestión Contractual, define y administra los modelos de Acuerdos de Confidencialidad y de Intercambio de Información con terceros, incluyendo los compromisos adquiridos, la prohibición de divulgación no autorizada, las obligaciones de eliminación de la información una vez cumplida su finalidad y la entrega de soportes que evidencien dicha eliminación. Cuando sea necesario, se solicita el acompañamiento de las dependencias competentes.
- Todo intercambio de información con terceros debe estar soportado en contratos o convenios que incluyan Acuerdos de Confidencialidad. Cuando la naturaleza del intercambio lo requiera, se debe elaborar un anexo técnico, generado por el área solicitante con el acompañamiento de la Oficina de Tecnologías de la Información, la Subdirección de Seguimiento y las áreas correspondientes de la entidad externa, en el cual se detallen los datos a intercambiar, canales, mecanismos de transferencia, controles de seguridad, flujo de información, autorizaciones, autenticación y disposiciones para la eliminación de la información. Se privilegia, siempre que sea posible, el intercambio automatizado con mínima intervención humana.
- La Oficina de Tecnologías de la Información a través del Profesional Especializado de Seguridad Informática define y habilita los mecanismos tecnológicos para el intercambio seguro de información digital, garantizando la confidencialidad, integridad y disponibilidad de la información, en especial aquella relacionada con las personas sujeto de atención de la ARN. Adicionalmente, se debe acordar con la entidad externa el uso de mecanismos de cifrado y anonimización si es posible (según la naturaleza de la solicitud), para los archivos que contengan información pública clasificada o reservada, datos sensibles o datos privados, a fin de evitar accesos no autorizados durante el proceso de intercambio.
- Los supervisores de convenios y contratos deben verificar que el intercambio de información de la ARN con entidades externas se realice conforme a esta política, a los acuerdos suscritos y a los mecanismos definidos, asegurando la trazabilidad de las transacciones, la aplicación del principio de mínima información necesaria y el cumplimiento de la normativa de protección de datos personales.
- Los propietarios de los activos de información deben autorizar las solicitudes de envío o recepción de información a terceros, salvo en los casos derivados

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		CÓDIGO: TI-M-01
		FECHA 2026-09-08	VERSIÓN V- 14

de obligaciones legales, requerimientos de entes de control o disposiciones normativas vigentes.

- Los terceros que reciban información de la ARN deben garantizar su manejo adecuado conforme a las políticas de seguridad de la entidad, las condiciones contractuales establecidas y la TI-G-01 Guía de Intercambio de Información.
- La Oficina de Tecnologías de la Información debe disponer de herramientas de monitoreo orientadas a la prevención de fuga de información y a la detección de comportamientos anómalos, las cuales generan alertas que son revisadas periódicamente para la adopción de las acciones correspondientes.
- La ARN debe habilitar las herramientas y controles para proteger la transferencia de información frente a interceptación, copia, modificación, redireccionamiento o destrucción no autorizada.
- Los usuarios deben utilizar exclusivamente los medios institucionales autorizados (carpetas compartidas, SharePoint u otros definidos por la entidad) para el manejo de información sensible. No está permitido el uso de correos electrónicos personales, aplicaciones de mensajería instantánea, llamadas telefónicas o servicios de almacenamiento en la nube no autorizados para el intercambio de información sensible de la ARN.
- Cuando la información intercambiada sea utilizada para estudios, investigaciones o productos académicos, se debe dar cumplimiento a los procedimientos y guías institucionales sobre propiedad intelectual e investigación aplicables.

La gestión, creación, modificación e inactivación de usuarios externos en aplicativos y servicios de la ARN es responsabilidad de los supervisores de los contratos o convenios, quienes deben solicitar oportunamente los ajustes correspondientes a través de los canales institucionales definidos, garantizando la suscripción previa de los Acuerdos de Confidencialidad.

La ARN cuenta con una TI-G-01 Guía para intercambio de información, en la cual establece los mecanismos operativos para efectuar los intercambios de información de forma segura y controlada, en cumplimiento de esta política y del SGSI

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

5.3.9 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, para reducir los riesgos generados por el error humano o el uso inadecuado de los recursos y manejo inapropiado de la información por acción u omisión.

- Todo empleado público al ingresar debe firma un compromiso de confidencialidad. Los contratistas, dentro del anexo técnico, se encuentra el clausulado de confidencialidad.
- Todos los empleados públicos y contratistas deben asistir a la inducción, reinducción y jornadas de sensibilización efectuadas por la entidad para el SGSI.
- Cada empleado público y contratista debe ser responsable de conocer y cumplir las Políticas de Seguridad de la Información.
- Cada empleado público o contratista debe realizar el curso de Seguridad de la Información dispuesto por la entidad.

5.3.10 Política de Teletrabajo

La ARN establece lineamientos para la implementación del Teletrabajo de conformidad con lo establecido en el TH-M-01 Manual de Teletrabajo.

Las actividades realizadas se deben llevar a cabo cumpliendo las políticas y controles de seguridad y privacidad de la información de la ARN.

Los recursos tecnológicos y organizacionales para la adopción del modelo de teletrabajo deben permitir el cumplimiento de los intereses y necesidades de la entidad, considerando los riesgos y su respectiva gestión.

La ARN debe proveer los mecanismos de seguridad lógica a los equipos de la entidad para el desarrollo de las actividades de teletrabajo, con el fin de conservar las características de integridad, disponibilidad y confidencialidad de la información.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

En caso de pérdida o hurto de un equipo en el cual se lleven actividades del modelo de teletrabajo, debe ser responsabilidad del empleado público informar de forma inmediata a través del centro de servicios.

5.3.11 Política de operaciones y de redes

- La Oficina de Tecnologías de la Información debe operar y administrar los recursos tecnológicos que soportan la gestión institucional de la ARN implementando acciones para el manejo de los cambios en la infraestructura, aplicativos, sistemas de información y servicios tecnológicos que son propios o soportados por terceros y/o proveedores de acuerdo con lo establecido en la TI-G-09 guía de gestión de cambios de tecnologías de la información.
- La Oficina de Tecnologías de la Información debe establecer y mantener las responsabilidades y procedimientos para la gestión y operación de los recursos de infraestructura tecnológica y de la información.
- Los empleados públicos, contratistas y terceros deben abstenerse de abrir, ejecutar o descargar archivos y/o documentos provenientes de fuentes desconocidas, en especial aquellos contenidos en medios de almacenamiento externo o recibidos por correo electrónico. En caso de requerir la información se debe solicitar autorización a la Oficina de Tecnologías de la Información mediante solicitud al centro de servicios.
- Todos los (las) empleados(as) públicos, contratistas o terceros que sospechen o detecten alguna infección por software malicioso deben notificar de inmediato el evento a través del centro de servicios.
- Ningún empleado público y contratista o tercero puede ejercer actividades de administración sobre equipos asignados por la entidad. Los únicos autorizados para desarrollar esta función es la Oficina de Tecnologías de la Información.
- Se prohíbe la instalación y el uso de software no autorizado.

Protección contra código malicioso

La Oficina de Tecnologías de la Información debe:

- Contar y 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 últimas bases de datos de firmas del proveedor de servicios.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

- Asegurar que la información almacenada en la plataforma tecnológica de la ARN sea escaneada por el software antivirus autorizado o adoptado.

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 evento o incidente que se pueda presentar.
- 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.
- 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, con protocolos de conexión seguros y monitoreados.

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

Lineamientos:

- La Oficina de Tecnologías de la Información debe asegurar que los desarrollos interno 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 por la ARN, de acuerdo con lo descrito en el documento TI-G-06 Guía de desarrollo de software, para los desarrollos externos contratados con este objeto deben observar las obligaciones contractuales que le apliquen en termino de desarrollo seguro.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

- La Oficina de Tecnologías de la Información debe establecer y mantener ambientes separados de Desarrollo/Pruebas y Producción, dando el uso o funcionalidad correspondiente para cada ambiente.
- La Oficina de Tecnologías de la Información debe restringir el acceso a compiladores, editores y otros utilitarios destinados para modificación de software propio de la ARN o adquirido a terceros con el fin de evitar la modificación no autorizada y un eventual inadecuado funcionamiento.
- La Oficina de Tecnologías de la Información debe mantener la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información con el fin que estén actualizados.
- 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.

5.3.13 Política de control de acceso

- Para la protección de los activos de información, la ARN tiene establecido procedimientos y lineamientos para el control de acceso a la red, sistemas de información e infraestructura física (Instalaciones). Con el fin de mitigar los riesgos asociados al acceso no autorizado a la información.
- Todos los usuarios deben asumir la responsabilidad sobre la información física o digital que accedan y procesan dando un uso adecuado con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información.
- El acceso a datos personales debe limitarse al mínimo necesario para el cumplimiento de funciones / obligaciones y quedar registrado en los registros de auditoría.

De acceso a Internet

- El acceso a internet por parte de los(las) empleados(as) públicos, contratistas y externos, debe realizarse de acuerdo con el perfil de navegación definido por la Oficina de Tecnologías de la Información.
- Es responsabilidad de todos los empleados públicos y contratistas verificar los derechos de propiedad intelectual de cualquier material obtenido en Internet

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

(libros, artículos, informes, imágenes, software y sitios web) antes de su uso en estaciones de trabajo.

- Es responsabilidad de todos los empleados públicos y contratistas, no hacer uso ni descargar software no autorizado por parte de la Oficina de Tecnologías de la Información.

De los centros de procesamiento de datos

El acceso a los centros de datos debe ser debidamente controlado teniendo en cuenta los siguientes lineamientos:

- Los accesos y visitas a los centros de datos, por parte del personal autorizado, deben estar debidamente aprobados por el Coordinador de Infraestructura y Soporte, de lo cual debe quedar registro.
- Cuando un empleado público o contratista, con acceso a los centros de datos que finaliza su vinculación con la entidad, el Coordinador de Infraestructura debe de solicitar la revocación de estos quedando su respectivo registro.
- Los accesos y visitas a los centros de cableado, cuartos técnicos de los Grupos Territoriales, por parte del personal autorizado, se deben gestionar por medio de la herramienta dispuesta por la subdirección administrativa y en el caso de los grupos territoriales debe de contar con el acompañamiento de asistentes de información.
- Los acceso, visitas y retiro o ingreso de equipos a los centros de cableado, cuartos técnicos de la sede central, por parte del personal autorizado, se realiza por medio de la herramienta de gestión de la entidad y con el acompañamiento de la OTI.
- Todo ingreso o retiro de algún equipo de cómputo o comunicaciones desde o hacia los centros de datos, debe ser autorizado por el Coordinador de Infraestructura.

De los sistemas de información

- La Oficina de Tecnologías de la Información valida que los desarrollos internos de los sistemas de información cumplan con los requerimientos de seguridad adecuados para la protección de la información de la ARN siguiendo el documento TI-G-06 Guía de desarrollo de software, que detalla los requerimientos de seguridad para el desarrollo, pruebas, puesta en producción y mantenimiento de los sistemas de información.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

- Para adquisiciones de aplicativos de terceros, 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.
- La entidad definió 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.

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 credenciales que no sean propias.
- Todos los(las) empleados(as) públicos y contratistas son responsables de los registros y/o modificaciones de información que se hagan a nombre de su cuenta de usuario.
- Todas las contraseñas deben tener una longitud mínima de doce (12) caracteres que deben cumplir con las siguientes características: Incluir combinación de números, letras mayúsculas, letras minúsculas y caracteres especiales.
- Todas las cuentas de usuario bloqueadas por intentos fallidos, su reactivación se debe dar por parte del administrador o gestores del directorio activo, a través de un caso en la herramienta de gestión.
- Las contraseñas de acceso a los sistemas de información deben tener una caducidad periódica automática, de igual forma cualquier cambio extemporáneo de contraseña solamente puede ser solicitado por el titular de la cuenta o su jefe inmediato si el titular se encuentra ausente y/o por necesidad del servicio.
- Cuando un empleado público o contratista se retira de la ARN, todas las credenciales asignadas sobre los recursos informáticos otorgados deben ser inhabilitadas teniendo en cuenta la información entregada por las áreas encargada.
- Las cuentas de usuario en estado deshabilitado que cumplan un periodo de tres meses en dicho estado deben ser eliminadas por parte del administrador del directorio activo o a quien se le delegue.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

- 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.
- Los(las) empleados(as) y contratistas deben cerrar sesión en aplicaciones o sistemas de información al finalizar su uso. No se deben mantener listados de contraseñas en ningún tipo de archivo o medio de almacenamiento que puedan ser vulnerados o accedidos por usuarios no autorizados.
- Para el caso que la cuenta de usuario se encuentre involucrada en algún delito informático o delito, es responsabilidad solo del empleado público o contratista que tenga asignada esta cuenta.

Estaciones de trabajo

- Todas las estaciones de trabajo (físicas o virtuales) asignadas por la entidad deben tener una contraseña de ingreso y un protector de pantalla con contraseña y activación automática.
- Cuando el empleado público o contratista se ausente o al finalizar jornada de trabajo, debe bloquear el acceso a equipo.
- 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.
- El mecanismo de autenticación para el acceso a la red de la entidad debe requerir únicamente las credenciales autorizadas (usuario y contraseña), sin solicitar información adicional distinta a dichos datos.
- La autenticación del usuario debe ser requerida cada vez que el equipo se encienda, reinicie, bloquee o después de aparecer el protector de pantalla.

5.3.14 Política de seguridad física y del entorno

Acceso a las instalaciones

- Todos los(las) empleados(as) públicos y contratistas que cuenten con el carnet institucional, deben portarlo de forma visible durante su permanencia en las instalaciones de la ARN.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

Control de áreas seguras

- Los visitantes que realicen actividades de mantenimiento, obras o infraestructura deben estar previamente autorizados, cumplir con las medidas de seguridad pertinentes, registrarse permaneciendo acompañados por personal autorizado durante toda su estancia para el desarrollo adecuado de sus actividades.
- Las puertas y ventanas de áreas seguras deben permanecer cerradas y bloqueadas cuando estén desocupadas.
- Está prohibido fumar, ingresar comidas, bebidas, armas o manipular equipos sin autorización previa.
- Se prohíbe alterar configuraciones, etiquetas o conexiones físicas de los sistemas de información.
- Todo acceso o actividad en estos espacios debe ser registrado y monitoreado por el personal de vigilancia.
- Los puntos de acceso deben contar con vigilancia o sistemas equivalentes para controlar el ingreso.
- La vigilancia privada debe verificar el estado de las puertas en centros de cableado y dejar constancia de cualquier incidencia.
- El personal de vigilancia privada debe operar bajo los estándares de las normas ISO 9001:2015, ISO 45001, ISO 18788, ISO 14001 e ISO 27001, garantizando la calidad y sostenibilidad en la seguridad.
- 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.
- Todas las personas dentro de las instalaciones deben actuar de manera responsable, respetando los protocolos y normativas establecidas por la entidad para proteger la infraestructura y garantizar un entorno seguro.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

5.3.15 Política de pantalla y escritorio limpio

- Se debe conservar el escritorio libre de información de la ARN (documentos físicos o unidades de almacenamiento externo) y conservar la pantalla del equipo de cómputo despejada de archivos.
- Los archivos que se trabajen en los equipos de cómputo deben ser almacenados en el OneDrive® y SharePoint Online de Microsoft 365® institucional o Carpeta compartida dispuesta para tal fin.
- No se deben exponer a personal no autorizado, documentos o datos reservados o clasificados, datos de la entidad, como: nombres de usuario, contraseñas, direcciones IP, información pública reservada o pública clasificada, listas de usuario o población objeto, archivos de propiedad intelectual, datos personales de los empleados Públicos o Contratistas y/o cualquier información importante o sensible para la ARN.
- Adoptar las medidas preventivas necesarias para el uso de sustancias, líquidos u objetos en el escritorio, ya que estos pueden dañar los equipos, así como la documentación y reducir el espacio de trabajo establecido por ley.
- La estación de trabajo y los equipos asignados constituyen activos de la entidad; en consecuencia, el usuario debe usarlos conforme a las políticas establecidas y reconoce que no son de su propiedad, en todo caso, la persona responsable del equipo debe evitar su uso para temas que no sean en cumplimiento de sus funciones u obligaciones.

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.
- Se debe guardar bajo llave o mantener en un sitio de acceso restringido, los documentos en formato físico o en dispositivos removibles que contengan información calificada como pública CLASIFICADA y/o pública RESERVADA

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

5.3.16 Políticas de criptografía

- La ARN protege la confidencialidad, disponibilidad e integridad de la información de la Entidad, pública RESERVADA o pública CLASIFICADA mediante el cifrado de datos durante su tratamiento
- La ARN debe implementar el uso de herramientas y técnicas criptográficas, con el fin de fortalecer la seguridad de la información, siguiendo lo indicado en documento TI-G-24 Guía custodia de llaves criptográficas.
- 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 debe utilizar controles criptográficos en los siguientes casos:
 - Para la custodia de las llaves criptográficas utilizadas en la entidad.
 - Para la transmisión de información pública RESERVADA o pública CLASIFICADA, fuera de la Entidad.
 - En la protección de la información a resguardar, cuando así lo establezca la 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

- Las herramientas de comunicación adoptadas por la entidad deben usar 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 en 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 pública CLASIFICADA o pública RESERVADA, bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

- La Oficina de Tecnologías de la Información debe proveer las herramientas de cifrado de datos a los usuarios, previa solicitud formal del propietario del activo de información, a través de un caso registrado en la herramienta de gestión.

Para los sistemas de información desarrollados internamente, la Oficina de Tecnologías de la Información debe evaluar e implementar métodos de cifrado adecuados para la información pública CLASIFICADA o pública RESERVADA, garantizando su confidencialidad e integridad. En el caso de información pública, se aplican medidas proporcionales de protección según el contexto. El diseño debe considerar el impacto del cifrado en el rendimiento del sistema, buscando siempre el equilibrio entre seguridad y eficiencia.

5.3.17 Política de relación con proveedores

La Agencia para la Reincorporación y la Normalización (ARN) establece la presente Política de Relación con Proveedores como parte integral de su Sistema de Gestión de Seguridad de la Información (SGSI), con el propósito de asegurar que los riesgos de seguridad de la información derivados de la relación con terceros, proveedores, contratistas y aliados estratégicos sean identificados, evaluados, tratados y monitoreados de manera adecuada.

El Grupo de Gestión Contractual debe incorporar en las minutas de los contratos, convenios demás instrumentos jurídicos, cláusulas y obligaciones relacionadas con la seguridad de la información, la protección de datos personales, los derechos de propiedad intelectual y los derechos de autor, las cuales debe ser divulgadas a los proveedores y terceros a través de los supervisores de contratos garantizando su conocimiento y cumplimiento durante toda la vigencia contractual.

Previo a la suscripción de contratos, convenios o acuerdos de cualquier naturaleza, el Grupo de Gestión Contractual debe asegurar que se identifiquen y evalúen los riesgos asociados a la seguridad y privacidad de la información, incluyendo los compromisos de confidencialidad, las condiciones de acceso, uso, almacenamiento, transmisión y eliminación de la información, así como la obligación de cumplir las políticas de seguridad de la información de la ARN y la normativa aplicable.

La Oficina de Tecnologías de la Información debe establecer, implementar y documentar controles técnicos cuando un tercero o proveedor requiera tener accesos a información sistemas, aplicativos, redes o infraestructura tecnológica de la ARN, de conformidad con la TI-F-01 Solicitud de usuarios y/o recursos tecnológicos, garantizando el principio de mínimo privilegio y la segregación de funciones.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

- Los supervisores de contratos son los responsables de verificar periódicamente el cumplimiento de Acuerdos de Nivel de Servicio y de las obligaciones contractuales relacionadas con la seguridad de la información, así como de velar por el cumplimiento de las políticas de seguridad de la información durante la ejecución del contrato, informando oportunamente cualquier desviación o incidente de seguridad.
- La Oficina de Tecnologías de la Información debe definir y aplicar las acciones para la gestión de cambios en infraestructura, aplicativos y servicios tecnológicos soportados por terceros y/o proveedores, conforme a lo establecido en la TI-G-09 Guía de gestión de cambios de tecnologías de la información, asegurando que dichos cambios no comprometan la seguridad de la información ni la continuidad de los servicios.

La relación con proveedores debe contemplar mecanismos para la terminación segura de los contratos, incluyendo la revocatoria de accesos, la devolución o eliminación de la información de la ARN, la verificación del cumplimiento de las obligaciones de confidencialidad posteriores a la finalización contractual y la preservación de evidencias cuando aplique.

5.3.18 Política de gestión de incidentes de seguridad de la información

- Todos los servidores públicos, contratistas y proveedores que tengan acceso a la información Institucional, deben ser sensibilizados en temas de Seguridad de la Información, para que reporten los eventos o incidentes por medio de los mecanismos y lineamientos establecidos en el documento TI-G-04 guía para la gestión de incidentes de seguridad.
- La Oficina de Tecnologías de la Información debe desarrollar y mantener la documentación necesaria para la gestión de los incidentes de seguridad de la información en la ARN.
- Para la gestión de incidentes de seguridad de la información se debe cumplir con lo establecido en los lineamientos y procedimientos dispuestos para este fin.
- La Oficina de Tecnologías de la Información debe mantener contacto con grupos de interés especiales como MINTIC, COLCERT, CSIRT entre otros, los cuales le permitan tener conocimiento sobre las mejores prácticas y mantenerse actualizado con la información de seguridad relevante, que ayude a prevenir incidentes de seguridad.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

5.3.19 Política de gestión de vulnerabilidades

- La ARN, a través de la Oficina de Tecnologías de la Información debe verificar la existencia de vulnerabilidades técnicas, apoyándose en herramientas tecnológicas para su identificación, sobre los activos de información de tipo infraestructura que son definidos para la realización periódica de pruebas de vulnerabilidades, gestionando su remediación. Con base en lo establecido en la TI-G-10 Guía de Gestión de Vulnerabilidades.
- Los empleados públicos y contratistas deben reportar 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

- La Oficina de Tecnologías de la Información de la Información debe realizar las actividades necesarias para la ejecución de las pruebas de vulnerabilidades a través de entes externos e independiente a la entidad, con el fin de tener imparcialidad y objetividad.
- La Oficina de Tecnologías de la Información de la Información, debe generar un cronograma de las actividades para la remediación de vulnerabilidades durante la vigencia.
- El ente externo que ejecute las pruebas de vulnerabilidades debe presentar informe de los resultados obtenidos durante la vigencia.
- La Oficina de Tecnologías de la Información debe generar, ejecutar y monitorear los planes de acción para la remediación de las vulnerabilidades técnicas detectadas en las plataformas tecnológicas.
- La Oficina de Tecnologías de la información debe identificar el nivel de exposición de vulnerabilidades técnicas en la infraestructura de la entidad de acuerdo con lo indicado en la TI-G-10 guía de gestión de vulnerabilidades.

5.3.20 Política de continuidad del negocio

La Agencia para la Reincorporación y la Normalización (ARN) adopta herramientas y mecanismos para garantizar una respuesta institucional efectiva y eficiente ante emergencias o crisis, con el objetivo de restablecer sus funciones y

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

servicios críticos en el menor tiempo posible. Esta política se fundamenta en la familia de normas ISO 27001 e ISO 22301, así como en la normativa legal aplicable en materia de análisis y manejo de riesgos, seguridad digital, gestión de tecnologías de la información y gestión documental.

Para responder a situaciones de crisis que afecten la continuidad del negocio, la ARN establece los siguientes lineamientos:

Plan de Continuidad del Negocio (PCN):

- Define los procedimientos para el restablecimiento oportuno de procesos críticos, infraestructura esencial y protección del personal (empleados(as) públicos y contratistas) ante eventos de interrupción o desastre.
- Los tiempos de recuperación deben cumplir con los márgenes establecidos en el análisis de impacto de continuidad del negocio (BIA, por sus siglas en inglés).

Capacitación y sensibilización:

- Todos los(las) empleados(as) públicos y contratistas reciben formación continua para fortalecer sus competencias en materia de continuidad del negocio y garantizar el entendimiento de sus responsabilidades en este marco.

Líderes de continuidad:

- Cada líder de proceso debe designar un Líder de Continuidad responsable de coordinar las actividades relacionadas con la gestión de continuidad del negocio dentro de su área.

Revisión y actualización del plan de continuidad de negocio:

- El Plan de Continuidad de Negocio es revisado y actualizado como mínimo una (1) vez al año o antes, en caso de que se identifiquen cambios significativos o necesidades críticas.
- Las actualizaciones se priorizarán según la criticidad de las fuentes de cambio: aquellas de alta importancia deben implementarse de inmediato, mientras que otras pueden integrarse en la revisión anual.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

Análisis de riesgos e impacto:

- Se realiza un análisis anual de riesgos y del impacto en la continuidad del negocio, conforme a lo establecido en el Manual de Gestión del Riesgo y el Plan de Continuidad de Negocio de la Entidad.
- Las estrategias de continuidad son revisadas cada vez que el líder del proceso lo considere necesario o como resultado de un análisis de riesgos actualizado.

Planes complementarios:

- Además del Plan de Continuidad de Negocio, la ARN debe contar con los siguientes instrumentos, que también se revisan anualmente o antes si es necesario:
 - Plan de Emergencias.
 - Plan de Recuperación de Desastres (PRD).
 - Plan de Manejo de Crisis.

Seguimiento y resultados:

- Los resultados de la gestión de continuidad del negocio y su seguimiento son presentados periódicamente en el Comité Institucional de Gestión y Desempeño. Este comité es responsable de validar ajustes y garantizar el cumplimiento de los objetivos de la política.

La ARN reitera su compromiso con la implementación de medidas integrales para asegurar la continuidad operativa, proteger a sus colaboradores y garantizar la prestación de servicios esenciales frente a cualquier contingencia que pueda afectar su operación

5.3.21 . Política de protección y tratamiento de datos personales

La ARN conforme a las disposiciones contenidas en la ley 1581 de 2012 establece dentro del DE-M-06 - Manual De Protección De Datos Personales los lineamientos de la política

5.3.22 Política Uso de dispositivos móviles

La Agencia para la Reincorporación y la Normalización (ARN) establece la presente Política de Uso de Dispositivos Móviles como parte de su Sistema de Gestión de Seguridad de la Información (SGSI), con el propósito de proteger la

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		CÓDIGO: TI-M-01
		FECHA 2026-09-08	VERSIÓN V- 14

confidencialidad, integridad y disponibilidad de la información institucional que sea procesada, almacenada o transmitida a través de estos dispositivos.

En caso de contar con dispositivos móviles asignados por la ARN, estos constituyen una herramienta de trabajo institucional y deben ser utilizados exclusivamente para el desarrollo de las funciones laborales o el cumplimiento de las obligaciones contractuales por parte de los(as) funcionarios(as) y contratistas. Todo dispositivo móvil que procese información de la ARN debe contar con mecanismos de autenticación seguros, tales como contraseña, PIN, patrón de desbloqueo, biometría u otros controles equivalentes definidos por la entidad. El uso de los dispositivos móviles de la ARN debe realizarse únicamente a través de redes seguras y confiables, aplicando las medidas de protección necesarias para prevenir accesos no autorizados, pérdida, alteración o divulgación indebida de la información almacenada o procesada en dichos dispositivos.

No está permitido instalar, configurar o utilizar en los dispositivos móviles de la ARN software, aplicaciones o servicios que no cuenten con la debida autorización institucional. Cualquier requerimiento de instalación o modificación debe ser gestionado a través de los canales definidos por la Oficina de Tecnologías de la Información. Los dispositivos móviles provistos por la ARN deben contar, como mínimo, con los siguientes controles de seguridad:

- Software antivirus o de protección de amenazas, debidamente licenciado y actualizado.
- Restricción de privilegios administrativos para los usuarios finales.
- Uso exclusivo de software licenciado o autorizado por la entidad.
- Mecanismos de seguridad que permitan la protección de la información en caso de pérdida, hurto o compromiso del dispositivo, tales como bloqueo remoto, borrado seguro u otros controles definidos por la Oficina de Tecnologías de la Información.

No está permitido transferir, almacenar o procesar información clasificada, reservada, sensible o datos personales de la ARN en dispositivos móviles personales ni en sitios redes o servicios no autorizados, tales como cafés internet, redes públicas, servicios de almacenamiento en la nube gratuitos, correos electrónicos personales, OneDrive® personal, aplicaciones de mensajería instantánea (como WhatsApp) o plataformas similares.

Se prohíbe el almacenamiento de información personal de los usuarios en los dispositivos móviles asignados por la ARN, así como la modificación de la configuración de seguridad establecida por la entidad. En caso de pérdida o hurto daño o cualquier incidente de seguridad que afecte un dispositivo móvil propiedad

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

de la ARN, el funcionario o contratista responsable debe reportar de manera inmediata la situación a su jefe inmediato o supervisor y a la Oficina de Tecnologías de la Información, a través del Centro de Servicios, por medio de la extensión 10999 o del correo electrónico soporte@reincorporacion.gov.co, con el fin de activar los procedimientos de gestión de incidentes de seguridad de la información.

El incumplimiento de la presente política da lugar a las acciones administrativas, contractuales o legales a que haya lugar, de conformidad con la normativa vigente y los acuerdos suscritos.

5.3.23 . Política para la utilización o desarrollo de la Inteligencia Artificial (IA)

- La ARN permite el uso de herramientas de inteligencia artificial licenciadas por la entidad, exclusivamente a través de cuentas institucionales y en entornos controlados.
- Se prohíbe el ingreso, tratamiento o divulgación de datos clasificados como sensibles, reservados o personales en plataformas de IA no autorizadas.
- Cada usuario es responsable de verificar la veracidad de la información generada por estas herramientas, mantener la confidencialidad de los datos a procesar o procesados y cumplir con el DE-M-06 Manual de protección de datos personales y las disposiciones establecidas por la Ley 1581 de 2012 (Ley de Protección de Datos Personales), el Decreto 1377 de 2013 (por el cual se reglamenta parcialmente la Ley 1581 de 2012) y las políticas institucionales de seguridad de la información y protección de datos personales.
- Cualquier iniciativa que contemple el uso de herramientas o modelos de inteligencia artificial por parte de las dependencias de la Entidad, debe ser evaluada y aprobada previamente por la Oficina de Tecnologías de la Información (OTI) y la Mesa de Seguridad de la Información. Esta revisión tiene como propósito asegurar que las soluciones propuestas cumplan con los lineamientos de seguridad establecidos en el presente manual, así como con los lineamientos institucionales de arquitectura, gobernanza y gestión del riesgo tecnológico. En este contexto, dichas instancias se solicitan, a través del centro de servicios, la realización de concepto de seguridad, pruebas de concepto (PoC) en caso de ser necesario y pruebas piloto como mecanismos de evaluación controlada, orientados a determinar la viabilidad funcional, técnica y de seguridad de las herramientas o modelos basados en IA. Estas

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

pruebas deben desarrollarse en entornos controlados, emplear datos no sensibles o debidamente anonimizados, y estar sujetas a seguimiento y supervisión por parte de los equipos responsables.

- La Entidad promueve el uso responsable de soluciones innovadoras basadas en IA, siempre que hayan sido evaluadas por los canales oficiales de revisión y cuenten con los avales necesarios para su eventual incorporación en el software autorizado de la ARN. Ninguna herramienta o modelo puede utilizarse en procesos misionales o de apoyo sin aprobación expresa de la OTI. Considerando que se trata de una herramienta no autorizada por la entidad, y siempre que sea indispensable para el desarrollo de las funciones y obligaciones de los servidores públicos y/o contratistas.

5.3.24 Política de Copia de seguridad (Backups)

- Se debe realizar Backups 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 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 sea designado.
- El grupo de Infraestructura y Soporte como responsable de ejecutar y mantener las copias de respaldo, debe contar con los recursos técnicos, documentales y de personal para realizar la validación y las restauraciones de la información cuando se requiera.
- Los (las) empleados(as) públicos y contratistas son responsables de la información almacenada en el equipo asignado, esta debe ser entregada al supervisor del contrato o jefe inmediato al finalizar su vinculación.

	MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: TI-M-01	
		FECHA 2026-09-08	VERSIÓN V- 14

- La Oficina de Tecnologías de la Información debe 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, teniendo en cuenta la programación del plan de generación de Backups.
- Las copias de seguridad y su retención están alineadas con las TRD del plan de preservación digital a largo plazo y se deben generar y resguardar en la herramienta de automatización de la tarea, de acuerdo con los planes diseñados por la Oficina de Tecnología de la Información

Copia de seguridad (Backups) de los archivos de usuario final de equipos de la ARN

- Los empleados públicos y contratistas deben ser responsables de la información almacenada en el equipo asignado y encargados de atender los lineamientos dispuestos por la OTI.
- La ARN debe contar con una herramienta licenciada para el respaldo de la información, actualmente es Microsoft 365 (software como servicio) incluye respaldo para Exchange Online, OneDrive® y SharePoint Online de Microsoft 365®. No cubre respaldo de otros elementos como chats de TEAMS, Planner, blog de notas.
- Se debe de disponer los archivos usados en el desarrollo de sus funciones y obligaciones contractuales, en la carpeta One Drive, Documentos o SharePoint.

Cuando finalice la vinculación del usuario con la ARN:

- La OTI debe realizar descarga de la última copia de respaldo de los archivos correspondiente a los usuarios desvinculados con la entidad, OneDrive® y correo electrónico de cada usuario, desde la plataforma de respaldo de servicios Microsoft 365, a el servidor dispuesto para este fin.

Las solicitudes de restauración de copia de seguridad (Backups) de los archivos de usuario final, deben ser tramitadas a través del Centro de Servicios por el jefe de Dependencia o Coordinador, anexando la una TI-F-01 Solicitud de Usuario y/o Recursos Tecnológicos dispuesto en SAPYG.