MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

TE-DR-006

Ministerio de Comercio, Industria y Turismo
Proceso
Junio - 2026

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Las políticas establecidas e incluidas en este documento son un componente fundamental para la gestión en seguridad y privacidad de la información del Ministerio de Comercio, Industria y Turismo, e incorpora los controles para la seguridad y privacidad de información implementados a través de los procesos, políticas y directrices institucionales.

Este documento es de propiedad del Ministerio y disponible para consulta de todos los interesados a través del sitio web institucional www.mincit.gov.co - Transparencia y Acceso a la Información Pública. La actualización del Manual de Políticas de Seguridad y Privacidad de Información se controla a través del Sistema Integrado de Gestión (en adelante SIG).

Las políticas de seguridad y privacidad de la Información deberán ser conocidas, aceptadas y cumplidas por todos los funcionarios, pasantes, contratistas, proveedores, Entidades del Sector Comercio, Industria y Turismo, Entidades públicas y privadas, y demás partes interesadas que tengan interacción con la plataforma tecnológica y sistemas de Información o de manera física a sus instalaciones y documentación.

En caso de incumplimiento en lo establecido en esta política por parte de funcionarios, pasantes, contratistas darán paso a la aplicación de las directrices internas para salvaguarda de la disponibilidad, confidencialidad e integridad de la información, sin perjuicio de la iniciación de instancias disciplinarias o contractuales a las que haya lugar.

Para reportar un evento sospechoso o un incidente de seguridad o de privacidad de la información relacionado con las políticas aquí detalladas, el Ministerio ha dispuesto los correos electrónicos info@mincit.gov.co de contacto para ciudadanos y soportetecnico@mincit.gov.co a nivel institucional.

1.1 OBJETIVO

Establecer y divulgar las Políticas de Seguridad y Privacidad de la Información del Ministerio de Comercio, Industria y Turismo a funcionarios, pasantes y contratistas, proveedores incluyendo personal suministrado por terceros que provean servicios al Ministerio, Entidades del Sector Comercio, Industria y Turismo, Entidades públicas y privadas y demás partes interesadas, esto con el fin de darlas a conocer para su respectivo cumplimiento.

1.2. ALCANCE

Las políticas de seguridad y privacidad de la información son aplicables para todos los aspectos administrativos, técnicos, tecnológicos y de control que deben ser cumplidas por directivos, funcionarios, contratistas, pasantes, proveedores, Entidades del Sector comercio, industria y turismo, Entidades públicas y privadas, ciudadanos y demás partes interesadas, que cumplan con alguna de las siguientes condiciones:

- Acceso a la información tanto física como lógica.
- Ingreso de manera física a las instalaciones o lógica a través de la plataforma tecnológica de la Entidad.
- Uso de equipos informáticos y de telecomunicaciones conectados a la plataforma tecnológica.
- Uso de los servicios informáticos dispuestos por la entidad a través de los canales digitales.
- Diseño, construcción, pruebas, implementación o uso de herramientas tecnológicas o servicios informáticos dispuestos por la entidad para el desarrollo de sus funciones.

1.3. VIGENCIA, REVISIÓN Y ACTUALIZACIÓN DEL MANUAL

La vigencia del Manual de Políticas de Seguridad y Privacidad de la Información aplica a partir de su aprobación por la Alta Dirección y publicación en el Sistema Integrado de Gestión y en el sitio web institucional www.mincit.gov.co - Transparencia y Acceso a la Información Pública. La revisión del contenido del Manual deberá realizar periódicamente; como mínimo una vez al año o cuando se presenten:

- Cambios organizacionales relacionados con la estructura orgánica, objetivos estratégicos o metas institucionales.
- Cambios en el entorno operativo de los procesos institucionales.
- Cambios en el entorno tecnológico de la entidad.
- Cambios en el entorno público y de la gestión administrativa de las instituciones.
- Cambios en el marco normativo o regulatorio interno y el que emita el Gobierno Nacional en materia de tecnologías de la información y comunicación, y que le sean aplicables a la gestión del Ministerio.
- Cambios como resultado de la gestión de continuidad operativa de la institución.

- Cualquier otro cambio que afecte o impacte en la seguridad y privacidad de la información del Ministerio.

1.4. TÉRMINOS Y DEFINICIONES

Se adoptan los términos y definiciones de la familia de normas técnica ISO 27000 vigentes, y de los estándares que se apliquen de acuerdo con el alcance de las políticas.

1.5 POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1.5.1 POLÍTICA

El Ministerio de Comercio, Industria y Turismo entendiendo la importancia de sus activos de información para el cumplimiento de su misión institucional está comprometido con la Seguridad y Privacidad de la Información mediante la implementación de políticas específicas para la seguridad de la información, ciberseguridad y protección de la privacidad, orientadas a proteger la confidencialidad, integridad y disponibilidad de los activos de información, en un entorno de confianza digital para el ejercicio de su misión con el Estado y los ciudadanos, acorde con el marco normativo de las Políticas de Gobierno y Seguridad Digital y las demás normas que apliquen, así como la reglamentación interna de sus procesos para el manejo de la información.

1.5.2 OBJETIVOS DE LA POLÍTICA

El Ministerio de Comercio, Industria y Turismo en su propósito de dar cumplimiento con la Política de Seguridad y Privacidad de la Información, establece los siguientes objetivos:
• Definir las directrices y políticas de seguridad y privacidad con el fin de salvaguardar los activos de información y protección de los datos personales en los procesos del Ministerio.
• Promover el manejo responsable de los activos de información de la Entidad.
• Evaluar el nivel de madurez y de eficacia de la gestión de la seguridad y privacidad de la información, mediante la mejorar continua de la seguridad y privacidad de la información, como resultado las evaluaciones internas, revisiones y aplicación de buenas prácticas en materia de seguridad de la información y protección de datos.

1.5.3 COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección del Ministerio está comprometida en:

• Apoyar y liderar La implementación, mantenimiento y mejora de la Seguridad y Privacidad de la Información;
• Revisar de manera periódica la Política Seguridad y Privacidad de la Información para que sea acorde con los lineamientos en la materia y la gestión institucional.
• Garantizar los recursos necesarios (tecnológicos y talento humano calificado) para implementar y mantener la Seguridad y Privacidad de la Información;
• Articular con los procesos institucionales la seguridad y Privacidad de la Información;
• Implementar los controles tecnológicos necesarios para la protección de los activos de información y reducir la materialización riesgos.

1.5.4 ALCANCE DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Política de Seguridad y Privacidad de la Información comprende a todos los procesos institucionales y activos de información, y aplica para todos los funcionarios, contratistas y terceros, conforme a los lineamientos de las Políticas de Gobierno y Seguridad Digital y requisitos interna para el manejo de la información de los procesos.

1.5.5 APLICABILIDAD

La Política de Seguridad y Privacidad de la Información, sus objetivos, manuales, procedimientos y documentos derivados o complementarios aplican a todos los procesos institucionales, servidores públicos, contratistas y terceros del Ministerio de Comercio, Industria y Turismo.

El incumplimiento de la Política de Seguridad y Privacidad de la Información y/o de sus lineamientos derivados, traerá consigo, las responsabilidades y consecuencias legales que apliquen a la normativa del Ministerio de Comercio, Industria y Turismo.

2. POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Política general de seguridad y privacidad de la información del Ministerio de Comercio, Industria y Turismo establece el compromiso de asegurar la salvaguarda de la información institucional, implementando los mecanismos y controles adecuados para garantizar su confidencialidad, integridad, disponibilidad y privacidad de la información, con el fin de mantener la continuidad de las operaciones del Ministerio. Los mecanismos y controles implementados responden al alcance de las políticas específicas y su aplicación a nivel institucional.

2.1. POLÍTICAS DE CONTROL ORGANIZACIONAL

2.1.1. Políticas para la seguridad de la información

ISO/IEC 27001:2022 ANEXO A.1.	ISO/IEC 27001:2013 ANEXO A.	DESCRIPCIÓN ANEXO A.1.
5.1. Políticas para la seguridad de la información	A.5.1.1. Políticas para la seguridad de la información. A.5.1.2. Revisión de las políticas para la seguridad de la información	La política de seguridad de la información y las políticas específicas asociadas deben ser definidas, aprobadas por la dirección, publicadas, comunicadas y reconocidas por el personal pertinente y partes interesadas pertinentes y revisadas a intervalos planificados y cuando ocurran cambios significativos en la organización.

Para el cumplimiento de la Política de Seguridad y Privacidad de la información se debe partir del Decreto 210 de 2003 y sus decretos reglamentarios que determinan la Estructura Orgánica del Ministerio, sus funciones y alcance de gestión mediante las cuales se establecen las políticas, lineamiento y manuales institucionales que tienen relación con la seguridad de la información y protección de datos, que se relacionan a continuación:

- Políticas del Modelo Integrado de Planeación y Gestión (MIPG)
- Política y Metodología para la Administración de Riesgos y Oportunidades
- Política de Gestión de Documentos Electrónicos
- Política Institucional de Servicio al Ciudadano
- Política de Participación Ciudadana
- Política de Operación Contable
- Política de Información y Comunicación
- Manual de Funciones Manual específico de funciones y competencias laborales MinCIT
- Manuales de contratación del MinCIT
- Manual de Políticas Contables
- Manual de Protección de Datos Personales
- Manual de Caracterización de Usuarios MinCIT
- Manual de Supervisión de Patrimonios Autónomos
- Manual Operativo del Modelo Integrado de Planeación y Gestión
- Manual Operativo del Sistema Integrado de Gestión
- Manual - Guía de Lenguaje Claro

2.1.2.Organización de la seguridad de la información

ISO/IEC 27001:2022 ANEXO A.1.	ISO/IEC 27001:2013 ANEXO A.	DESCRIPCIÓN ANEXO A.1.
A 5.2. Roles y responsabilidades para la seguridad de la información	A.6.1.1. Roles y responsabilidades para la seguridad de la información	Los roles y responsabilidad de seguridad de la información se deben definir y asignar de acuerdo con las necesidades de la organización.
A 5.3 Segregación de deberes	A.6.1.2. Separación de deberes	Los deberes y áreas de responsabilidad en conflicto deberían segregarse.
A 5.4. Responsabilidades de la Dirección	A.7.2.1. Responsabilidades de la dirección	La Alta Dirección debe exigir a todo el personal la aplicación de la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y los procedimientos específicos de la organización en los aspectos correspondientes.
A 5.5. Contacto con las autoridades	A.6.1.3. Contacto con las autoridades	La organización debe establecer y mantener contacto con grupos de interés especial u otros foros y asociaciones profesionales especializados en Seguridad.
A 5.6. Contacto con grupos de interés especial	A.6.1.4. Contacto con grupos de interés especial	La organización debe establecer y mantener contacto con las autoridades pertinentes.

2.1.2.1. Roles y Responsabilidades

El Ministerio de Comercio, Industria y Turismo - MinCIT define los roles y responsabilidades para la implementación de la Seguridad y Privacidad de la Información conforme con los lineamientos del Modelo Seguridad y Privacidad de la Información de la Política de Gobierno Digital y lineamientos de la Política de Seguridad Digital.
Las decisiones sobre las Políticas de Seguridad y Privacidad de la Información son tomadas por el Comité Institucional de Desempeño.

2.1.2.2 Segregación de Deberes

La separación de deberes define los roles, responsabilidades y niveles de autoridad de la seguridad y privacidad de la información a través de:

- **Manual de Funciones y Competencias Laborales**

La Gestión del Talento Humano asegura que la planta de personal sea vinculada atendiendo los requerimientos funcionales de los procesos institucionales acorde con los requerimientos funcionales de las áreas:

- El personal de la Entidad que realiza labores funcionales sobre la información, la infraestructura física o tecnológica, sean estas críticas o no, no pueden tener a su cargo labores de administración técnica, sobre la plataforma tecnológica (servidores, redes y comunicaciones o servicios tecnológicos y de aplicación).

- El personal funcional de la Oficina de Sistemas de Información (OSI) no debe tener decisión sobre los datos que se procesan en los sistemas de información de la entidad.

- Manual de Contratación del Ministerio

La Gestión Contractual asegura que la adquisición de bienes y servicios para apoyo a la gestión institucional se lleve a cabo en coordinación con los procesos y el Plan Anual de Adquisiciones:

El personal contratista y proveedores de servicios de tecnologías de información y comunicación, consultorías y asesorías, seguridad y vigilancia, mantenimiento áreas físicas y seguros, tendrá acceso a la información y sistemas de información requeridos en el marco de su objeto contractual.

Los Supervisiones de contratos deben asegurar que la información y los accesos físicos y lógicos requeridos por contratistas y proveedores sean coordinados con las áreas pertinentes.

2.1.2.3. Responsabilidades de la Dirección

• Comité Institucional de Gestión y Desempeño (CIGD)
La Alta Dirección representada en el CIGD asegura que se implementen los requisitos establecidos en la Política de Gobierno Digital, orientando la gestión y recursos de la seguridad y privacidad de la información en la Entidad y Sector Comercio, Industria y Turismo acorde con el alcance sectorial.

• Comité Institucional de Control Interno (CICI)
La Alta Dirección representada en el CICI evalúa la gestión institucional en la implementación de controles para la mitigación de riesgos de seguridad de la información, protección de datos y seguridad digital acorde con el alcance de la gestión tecnológica y demás procesos institucionales.

2.1.2.4. Contacto con las Autoridades y Grupos de Interés Especial

El Ministerio acorde con la estrategia de seguridad digital del Estado y con el fin de asegurar la disponibilidad, integridad, confidencialidad y privacidad de los activos de información de la entidad o del sector acorde con el alcance sectorial, mantiene contacto con autoridades cibernéticas y grupos de interés especial mediante los canales de contacto público o chats sectoriales establecidos, y designa a la Jefe de la Oficina La Oficina de Sistemas de Información para articular y coordinar las actividades o acciones que se requieren en materia de seguridad de la información, ciberseguridad y seguridad digital.

2.1.3.Inteligencia de Amenazas

ISO/IEC 27001:2022 ANEXO A.1.	ISO/IEC 27001:2013 ANEXO A.	DESCRIPCIÓN ANEXO A.1.
A 5.7. Inteligencia de Amenazas	NUEVO	La información relativa a las amenazas a la seguridad de la información se debe recopilar y analizar para producir inteligencia de las amenazas.

El Ministerio a través de la Oficina de Sistemas de Información gestiona los servicios y plataforma tecnológica para contar en tiempo real con el monitoreo de la infraestructura y servicios tecnológicos, gestionar eventos, incidentes y vulnerabilidades, implementar remediaciones que permitan asegurar la disponibilidad, integridad, confidencialidad y privacidad de los activos de información de la entidad o del sector acorde con el alcance sectorial.

El PETI – Plan Estratégico de Tecnologías de Información incorpora las iniciativas en materia de seguridad digital y el PAA – Plan Anual de Adquisiciones incorpora la programación de la adquisición de los bienes y servicios acorde con las necesidades de hardware, software, licencias y personal.

La Supervisión contractual verifica que los bienes y servicios adquiridos cumplan con los ANS – Acuerdos de Servicios pactados.

2.1.4.Gestión de Proyectos de TI

ISO/IEC 27001:2022 ANEXO A.1.	ISO/IEC 27001:2013 ANEXO A.	DESCRIPCIÓN ANEXO A.1.
A 5.8. Seguridad de la información en la gestión de proyectos	A.6.1.5. Seguridad de la información en la gestión de proyectos A.14.1.1. Análisis y especificación de requisitos de seguridad de la información	Seguridad de la información se debe integrar en la gestión de proyectos.

La gestión de tecnológica establece la estrategia de Tecnologías de la Información acorde con el entorno de gobierno, institucional y sectorial, para el efecto:

- Articula la Estrategia Institucional con la gestión tecnológica.
- Implementa el PETI Plan Estratégico de Tecnologías de la Información.
- Evalúa los Proyectos Institucionales con alcance tecnológico.
- Incorpora los requisitos de seguridad y privacidad de la información, ciberseguridad y de seguridad digital requeridos para los proyectos.
- Evalúa los riesgos que puedan impactar la confidencialidad, privacidad, integridad y disponibilidad de la información de la Entidad, del sector o de procesos intersectoriales.

El PETI incorpora las iniciativas de proyectos institucionales o de articulación sectorial o intersectorial en los cuales se determina los requerimientos y recursos para su desarrollo e implementación de componentes tecnológicos (infraestructura tecnológica, software, hardware, almacenamiento, personal, seguridad digital, etc.).

2.1.5.Gestión de Activos de Información

ISO/IEC 27001:2022 ANEXO A.1.	ISO/IEC 27001:2013 ANEXO A.	DESCRIPCIÓN ANEXO A.1.
A 5.9. Inventario de Información y Otros Activos Asociados	A.8.1.1. Inventario de activos A.8.1.2. Propiedad de los activos	Se debe elaborar y mantener un inventario de la información y otros activos asociados, incluidos los propietarios.
A 5.10. Uso aceptable de la información y otros activos asociados	A.8.1.3. Uso aceptable de los activos A.8.2.3. Manejo de activos	Se deben identificar, documentar e implementar normas para el uso aceptable y procedimientos para el tratamiento de la información y otros activos asociados.
A 5.11. Devolución de activos	A.8.1.4. Devolución de activos	EL personal y otras partes interesadas, según corresponda, deben devolver todos los activos de la organización en su posesión al cambiar o terminar su empleo, contrato o acuerdo.

El MinCIT cuenta los lineamientos y procedimientos para gestionar los activos requeridos por los procesos para el manejo de la información gestionada de manera física, digital o electrónica y de uso de funcionarios, contratistas y/o proveedores.

2.1.5.1. Inventario de activos de información y otros activos asociados

Todo el personal del Ministerio sin importar su tipo de vinculación debe mantener periódicamente actualizado y al momento de su retiro de la Entidad los inventarios de bienes, archivos documentales, de activos de información o cualquier otro inventario que se genere en desarrollo de las funciones o de los objetos contractuales, que informe sobre el uso, manejo, disposición de la información institucional y componentes tecnológicos asociados.

Los inventarios que informan sobre activos de información institucionales son:

• Inventario de Bienes Institucionales, relaciona los bienes de hardware, software, físicos, y se actualizan conforme con las directrices y procedimientos de la Gestión Recursos Físicos.
• Inventario Documental, relaciona los registros documentales de archivo valorados por el área o documentos finales por valorar, conforme con las directrices y procedimientos de la Gestión Documental y la TRD – Tabla de Retención Documental del proceso y área ejecutora de la función u objeto contractual.
• Inventario de Activos de Información de Seguridad y Privacidad de la información, relaciona los activos por proceso conforme con las directrices y procedimientos de la Gestión de TI y el documento Guía Activos de Información.

- **Propiedad de los activos de información**

Todos los Activos de Información deben tener un propietario o responsable asociado.

Los Propietarios son los Líderes de los Procesos Institucionales y Supervisores contractuales.

Los Propietarios de los activos de información en cualquiera de sus tipos y disposición física o digital o electrónica son responsables de:

• Identificar, clasificar y actualizar los activos de información (hardware, software, información, de alojamiento y de imagen) relacionados con la información de sus respectivos procesos y áreas acorde con las directrices y requerimientos de actualización periódica de la gestión de recursos físicos, gestión documental y gestión tecnológica.
• Garantizar que se documenten los controles apropiados para guardar la confidencialidad, integridad, privacidad y disponibilidad de los activos de información y componentes tecnológicos asociados.

- **Custodios de los activos de información**

Todo el personal del Ministerio sin importar su tipo de vinculación es Custodio de activos de información y son responsables del adecuado uso, manejo y disposición de la información en los medios previstos por la entidad para su procesamiento, almacenamiento y disposición final, así como el acceso a los componentes tecnológicos asociados con la información.

- **Usuarios de los activos de información**

Todo el personal del Ministerio sin importar su tipo de vinculación es Custodio de la información y de los componentes tecnológicos o en medios de almacenamiento físico o virtuales asociados a la información y a los cuales tengan acceso físico, digital o electrónico para su procesamiento, uso, manejo y disposición en los medios de almacenamiento o archivo previstos por la entidad.

2.1.5.2. Uso aceptable de la información y otros activos asociados

Toda la información del Ministerio sin importar el tipo de soporte (físico, digital o electrónica) debe ser procesada y almacenada en los medios físicos o tecnológicos previstos por la entidad de acuerdo con su nivel de clasificación, de manera que se protejan las propiedades de confidencialidad, privacidad, integridad y disponibilidad.
El personal de la Entidad independiente del tipo de vinculación deberá tener en cuenta para el uso adecuado de los activos de información y otros activos asociados (hardware, software, almacenamiento en nube, equipos de comunicación móvil e instalaciones físicas):

i. No realizar cambios en la configuración del hardware o software de los equipos (computadores, portátiles, tablets o equipos de comunicación de red, telefónica o móvil) o de licencias de software de programas o aplicativos asignados para el desarrollo de sus funciones o del objeto contractual.

La Oficina de Sistemas de Información es la autorizada para:	- Instalar/desinstalar, configurar, dar soporte a los equipos que conforman la plataforma tecnológica, así como conceptuar su pertinencia u obsolescencia acorde con el entorno tecnológico y requerimientos de los procesos institucionales. - Realizar o coordinar con los proveedores de desarrollo y mantenimiento de aplicativos y sitios web los cambios o ajustes requeridos para el adecuado manejo de la información.
El Grupo Administrativa es el área autorizada para:	- Realizar el mantenimiento preventivo o correctivo a equipos de comunicación telefónica o móvil, de video vigilancia o de acceso físico, en coordinación con los proveedores de los respectivos servicios. - Coordinar con la Oficina de Sistemas de Información las actividades de los proveedores que requieran el acceso a los componentes tecnológicos asociados a tales servicios y que se encuentren dentro de la infraestructura tecnológica de la entidad.

ii. No realizar cambios en los registros documentales de archivo valorados o finales asociados con la TRD independientemente de su formato (físico, digital o electrónico) y su disposición de archivo en áreas de gestión o en Archivo Central o Bodegas Documentales en el Grupo de Gestión Documental.

El Grupo de Gestión Documental es el área autorizada para:	- Determinar la disposición final (física, digital o electrónica) de los registros documentales de archivo, - Determinar las condiciones de preservación y conservación acorde con los lineamientos de la AGN – Archivo General de la Nación y el entorno institucional. - Coordinar con la Oficina de Sistemas de Información la infraestructura tecnológica requerida por el entorno institucional para el adecuado manejo, almacenamiento y consulta de los registros documentales, así como los mecanismos de transferencia electrónica documental a la AGN o Entes de Control o Terceros autorizados para tratar la información en los registros documentales de archivo.

iii. Cumplir con los controles físicos y tecnológicos establecidos por la Entidad para la salvaguarda de la información:

- En equipos institucionales o personales utilizados por el personal del Ministerio sin importar su tipo de vinculación, que se encuentre en las oficinas de la entidad o autorizados en trabajo remoto.
- En áreas de archivo y áreas restringidas del Ministerio.
- Para el acceso, manejo y protección de la información física y digital.
- Para el acceso a los servicios de aplicación y sitios web dentro o fuera de la entidad.

2.1.5.3. Devolución de activos

El personal de la Entidad independiente del tipo de vinculación al finalizar su vinculación laboral o contrato deben hacer entrega de los activos de información y otros activos asociados con la información conforme con los procedimientos de la gestión de recursos físicos, gestión documental y gestión tecnológica:
- Computadores, portátiles, tablets y medios de almacenamiento,
- Registros documentales de archivo y demás documentos generados en desarrollo de las funciones y el objecto contractual.
- Accesos a la red, aplicativos o servicios corporativos como correo electrónico, almacenamiento en nube, tokens o dispositivos de firma digital.
- Equipos de comunicación móvil, tarjetas de acceso a instalaciones físicas, y demás activos suministrados para el desarrollo de las funciones o del objeto contractual y los ANS – acuerdos de nivel de servicio.

2.1.5.4. Clasificación y Etiquetado de Información

ISO/IEC 27001:2022 ANEXO A.1.	ISO/IEC 27001:2013 ANEXO A.	DESCRIPCIÓN ANEXO A.1.
A .5.12. Clasificación de la información	A.8.2.1. Clasificación de la información	La información se debe clasificar de acuerdo con las necesidades de seguridad de la información de la organización sobre la base de la confidencialidad, integridad, disponibilidad y los requisitos pertinentes de las partes interesadas.
A 5.13. Etiquetado de la información	A.8.2.2. Etiquetado de la información	Se debe elaborar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información de conformidad con el esquema de clasificación de información adoptado por la organización.

Toda información que se encuentre bajo responsabilidad del Ministerio debe ser identificada, clasificada y documentada acorde con los lineamientos de la AGN – Archivo General de la Nación y de transparencia y acceso a la información, las directrices y procedimientos del Sistema de Gestión Documental institucional.

Grupo de Gestión Documental	- Coordina y articula con los procesos la identificación de los registros de archivo documental en soporte físicos, digital o electrónico y su clasificación y etiquetado acorde con la normatividad aplicable, los lineamientos del documento Guía para el Etiquetado de Información y los requisitos de preservación, conservación y consulta pública, privada, o de reserva por parte de los usuarios internos, entes de control y partes interesadas. - Interioriza y apropia a todo el personal del Ministerio las directrices y procedimientos para la adecuada identificación y clasificación de la información.

2.1.6.Transferencia de Información

ISO/IEC 27001:2022 ANEXO A.1.	ISO/IEC 27001:2013 ANEXO A.	DESCRIPCIÓN ANEXO A.1.
A 5.14. Transferencia de información	A.13.2.1. Políticas y procedimientos de transferencia de información A.13.2.2. Acuerdos sobre transferencia de información A.13.2.3. Mensajería electrónica	Las reglas, procedimientos o acuerdos de transferencia de información deben estar vigentes para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes.

El Ministerio como propietario y custodio de la información (física, digital y electrónica) generada como resultado del desarrollo de las funciones institucionales y objetos contractuales, se reserva el derecho de su conservación o destrucción, dependiendo del nivel de criticidad definida y preservación histórica de la información acorde con los lineamientos de la AGN y directrices del Comité Institucional de Gestión y Desempeño en lo referente a la Gestión Documental.

Para la transferencia y transporte de información del Ministerio a otras entidades o partes interesadas internas o externas se realiza acorde con su clasificación y aprobación del Propietario del activo de Información, las condiciones de presentación y medios de entrega de transferencia o transporte.

La transferencia o transporte de información sensible o crítica deberá estar plenamente justificada y contar con la suscripción de un "Acuerdo de Confidencialidad", que detalle el objeto de la salida de información, el medio de transferencia y/o transporte, y uso final.

2.1.6.1. Información en medios físicos o electrónicos

Para la información impresa o en medios físicos, con respecto a su acceso, uso, transporte, almacenamiento y disposición final, se aplican las directrices del Comité Institucional de Gestión y Desempeño en lo referente a la Gestión Documental y los procedimientos del proceso Gestión Documental.

• Grupo de Gestión Documental, acorde con los lineamientos de la AGN – Archivo General de la Nación, las directrices y procedimientos del Sistema de Gestión Documental institucional es el área encargada de:

- Programa y coordina las Transferencias Primarias de los registros documentales de archivo acorde con las TRDs para su control y salvaguarda en el archivo central, y realizar las transferencias secundarias al AGN de los documentos de archivo que han cumplido sus tiempos de retención para su preservación histórica.
- Coordina con la Oficina de Sistemas de Información los medios o mecanismos para el transmisión o transporte de información – documentos digitales - en medio de almacenamiento externos o canales electrónicos a interesados internos o externos.
- Coordina con el Grupo Administrativa el transporte de medios de almacenamiento de registros documentales a instalaciones del ministerio o entrega a otras entidades o interesados autorizados.

- Coordina y verifica con los proveedores de los servicios de correspondencia y encomienda él envió de documentos de archivo o información del Ministerio con destino usuarios externos y partes interesadas, por los canales físicos o digitales contratados.

• Grupo Administrativa, conforme los procedimientos de la Gestión de Recursos Físicos, es el área encargada de:

- Opera las bodegas para el almacenamiento, conservación, control y manejo de los archivos y material documental del Ministerio en coordinación con el Grupo de Gestión Documental, y del suministro de bienes de consumo y devolutivos.
- Coordina la entrega de los medios para el transporte de archivos y material documental del Ministerio en coordinación con el Grupo de Gestión Documental y/o Oficina Sistemas de Información acorde con los requerimientos específicos de transporte de información y las condiciones de transporte pactadas con el proveedor del servicio.

Personal del Ministerio, para la gestión de la información en medios de almacenamiento en nube institucional, computadores, portátiles, discos duros u otros activos a cargo del personal de la entidad:

- Se compromete a mantener y salvaguardar la información contenida en el mismo, atendiendo las directrices para el ingreso o retiro de activos institucionales o personales, uso adecuado y protección de equipos fuera de las instalaciones de la entidad y copias de respaldo de la información en los medios de almacenamiento asignados por el Ministerio para la transferencia de información.
- Hará entrega o transferencia de la información al Grupo de Gestión Documental acorde con la TRD del área y proceso en el cual desarrollo sus funciones u objeto contractual.
- Hará entrega o devolución de los equipos y de más activos asignados, de acuerdo con el procedimiento Administración y Control de Bienes Devolutivos y de Consumo, y el documento Guía para el Manejo Administrativo de los Bienes de Propiedad de la Nación.

2.1.6.2. Información en medios electrónicos

Para la información soportada en medios electrónicos de propiedad del Ministerio, el personal de la Entidad independiente del tipo de vinculación es responsable de:

• Mantener actualizado el inventario de activos de información que identifique los propietarios y usuarios, el nivel de custodia y la criticidad de estos.
• Para la información soportada en registros documentales de archivo aplicar la clasificación y etiquetado acorde con nivel de criticidad y los lineamientos de conservación o destrucción de información del proceso Gestión Documental.
• La Oficina de Sistemas de Información es el área autorizada para aplicar técnicas de borrado seguro de medios de almacenamiento electrónico como parte del servicio de mantenimiento

preventivo y correctivo en equipos de usuario final institucionales y administración de servidores, así mismo coordina la disposición final de los medios a fin de asegurar la privacidad de la información.

2.1.7.Control de Accesos y Gestión de Contraseñas

ISO/IEC 27001:2022 ANEXO A.1.	ISO/IEC 27001:2013 ANEXO A.	DESCRIPCIÓN ANEXO A.1.
A 5.15. Control de Acceso	A 9.1.1. Política de control de acceso A 9.1.2. Acceso a redes y a servicios de red	Las normas para controlar el acceso físico y lógico a la información y otros activos asociados se deben establecer e implementar sobre la base en los requisitos de seguridad empresarial y de la información.
A 5.16. Gestión de Identidades	A.9.2.1. Registro y cancelación del registro de usuario	Se debe gestionar el ciclo de vida completo de las identidades.
A 5.17. Información de Autenticación	A.9.2.4. Gestión de información de autenticación secreta de usuarios A.9.3.1. Uso de información de autenticación secreta A.9.4.3. Sistemas de gestión de contraseñas	La asignación y gestión de la información de autenticación se debe controlar mediante un proceso de gestión, incluido el asesoramiento al personal sobre el manejo adecuado de la información de autenticación.
A 5.18. Derechos de Acceso	A.9.2.2. Suministro de acceso de usuarios A.9.2.5. Revisión de los derechos de acceso de usuarios A.9.2.6. Retiro o ajustes de los derechos de acceso	Los derechos de acceso a la información y otros activos asociados se deben aprovisionar, revisar, modificar y eliminar de acuerdo con la política y reglas específicas de la organización para el control de acceso.

2.1.7.1. Política para el control de acceso

El Ministerio implementa la gestión de accesos físicos y lógicos del personal de la entidad conforme al perfil de acceso establecidos para el ingreso, permanencia y retiro de las instalaciones físicas comunes y restringidas de equipos, vehículos y bienes de la entidad o bajo su custodia, así como del personal de proveedores de servicios tecnológico, logísticos, de transporte u otro específico, que se encuentren autorizados para realizar ingreso, instalación, mantenimiento o retiro de equipos de comunicaciones, servidores, equipos de usuario final y dispositivos, o cualquier otro bien o elemento o componente físico y/o tecnológico.

El ingreso al Ministerio se realiza mediante:

- Acceso a las áreas de oficina, bodegas, áreas restringidas

Con tarjeta de proximidad para funcionarios, pasantes, contratistas, proveedores y partes interesadas, previa autorización del Grupo Administrativa; o mediante autorización ante el Grupo Administrativa para el ingreso temporal o eventual de personal acorde con las necesidades institucionales. Ver: Políticas de Control Físico.

- Acceso a la plataforma tecnológica y servicios corporativas (correo electrónico, internet, aplicación y sitios web y almacenamientos)

Con usuario y contraseña entregada por la Oficina por la Oficina de Sistemas de Información a funcionarios, pasantes, contratistas, proveedores y partes interesadas.

2.1.7.2. Control de Accesos a redes y a servicios de red

El acceso a la red de datos del MinCIT se realiza con el nombre de usuario y contraseña asignados por la Oficina de Sistemas de Información a funcionarios, pasantes, contratistas y proveedores o partes interesadas quienes deben proteger y no compartir sus credenciales de acceso a la red y servicios de red (correo electrónico, red inalámbrica, aplicaciones, entre servicios tecnológicos) que le son conferidos de acuerdo con su perfil.

El personal del Ministerio es responsable del usuario y contraseña asignados, así como del acceso a la plataforma corporativa y servicios de aplicación y sitios web a los cuales se autorizada su conexión, y deben notificar a la Oficina de Sistemas de Información cuando se sospeche su uso por terceras personas.

2.1.7.3. Administración de cuentas de usuario y contraseñas

La Oficina de Sistemas de Información administra la asignación y revocatoria de cuentas de usuario y contraseñas asignadas a funcionarios, pasantes, contratistas, proveedores o partes interesadas; aplica el procedimiento Accesos a Servicios de TI que especifica la metodología para nombrar las cuentas de usuario y establecer las contraseñas (password).
Así mismo se precisa que las cuentas de usuario y contraseñas:

• Se establecen de acuerdo con los estándares y directrices definidas por la Oficina de Sistemas de Información, con el propósito de asegurar la identidad y acceso a las diferentes plataformas corporativas.
• Son de uso personal e intransferible y por ningún motivo se deben compartirse con otros usuarios o terceros no autorizados.
• No deben ser reveladas por vía telefónica, correo electrónico, o ser escritas en ningún medio, excepto cuando son entregadas en custodia, previa autorización del Jefe inmediato del funcionario o contratista y de la Oficina de Sistemas de Información.
• No se debe habilitar la opción "recordar clave en este equipo", que ofrecen los programas o aplicaciones o navegadores web, esto con el fin de limitar el acceso a los aplicativos a personas no autorizadas, especialmente en entornos de trabajo remoto con autorización a la plataforma tecnológica y aplicativos o sistemas de información de la entidad.
• Cualquier sospecha de uso no autorizado del usuario y contraseña asignados se debe reportar al correo electrónico soportetecnico@mincit.gov.co.

2.1.7.4. Gestión de Identidades - Autenticación de usuarios

La Oficina de Sistemas de Información asignará un nombre de usuario, una contraseña y una cuenta de correo electrónico a funcionarios, pasantes, contratistas o proveedores o partes interesadas, previa autorización de:
• El Grupo de Talento Humano, al ingreso del funcionario y pasante.
• El Grupo de Contratos para los contratistas y proveedores indicando la fecha de inicio y fecha de terminación del contrato y actividad específica.
• Los Supervisores de los contratistas o proveedores que requieran tener acceso a la red del ministerio como parte del desarrollo de su objeto contractual.
• Jefes del área – Ministro, Viceministro, Director, Subdirector o Coordinador de Grupo para la solicitud de acceso:
- Como invitado temporal a la red del ministerio por parte de terceros o partes interesadas en desarrollo de actividades relacionadas con la gestión institucional.
- A personal del área para el acceso a plataformas corporativas.

Para el caso de usuarios y contraseñas de acceso a plataformas no institucionales para el registro de información institucional, el Jefe área y usuarios del área son responsables del uso y manejo de dichas credenciales.

La Oficina de Sistemas de Información:	- Se reserva el derecho de realizar la verificación del uso de los accesos por parte de los diferentes usuarios. - Realizar cambios en los diferentes servicios tecnológicos que mejoren la seguridad de la red y del usuario - Proteger la información institucional y proteger al usuario de eventos o situaciones que vulneren la privacidad de datos personales - Implementar los mecanismos de autenticación en las plataformas corporativas, aplicaciones y sitios web institucionales, como el doble factor de autenticación o control de autenticación en dos pasos.

2.1.7.5. Cancelación de cuentas usuario y deshabilitación de usuarios

La Oficina de Sistemas de Información procederá a deshabilitar o inactivar la cuenta de usuario institucional y/o el usuario de acceso a servicios de aplicación o sitios web asignada a funcionarios, pasantes, contratistas o proveedores o partes interesadas, previa confirmación de desvinculación del personal, por parte del Grupo de Talento Humano o del Grupo de Contratos. Para usuarios invitados, el acceso a la red de datos se establecerá como "Invitado" y se mantendrá activo máximo 8 horas hábiles, y se deshabilitará con la confirmación del retiro del visitante por el área solicitante.

2.1.8. Gestión de Proveedores de Servicios y Cadena de Suministro

ISO/IEC 27001:2022 ANEXO A.1.	ISO/IEC 27001:2013 ANEXO A.	DESCRIPCIÓN ANEXO A.1.
A 5.19. Seguridad de la información para las relaciones con proveedores	A.15.1.1. Política de seguridad de la información para las relaciones con proveedores	Se deben definir e implementar procesos y procedimientos para gestionarlos riesgos de la información asociada con el uso de los productos o servicios del proveedor.
A 5.20. Abordar la seguridad de la información en los acuerdos con los proveedores	A.15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores	Los requisitos pertinentes de seguridad de la información se deben establecer y acordar con cada proveedor en función del tipo de relación con el proveedor.
A 5.21. Gestión de la seguridad de la información en la cadena de suministro de las TIC	A.15.1.3. Cadena de suministro de tecnología de información y comunicación	Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociada a la cadena de suministros de productos y servicios de TIC.
A 5.22. Seguimiento, Revisión y Gestión de Cambios de Servicios de Proveedores	A.15.1.1. Política de seguridad de la información para las relaciones con proveedores A.15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores	La organización debe monitorear, revisar, evaluar y gestionar regularmente el cambio en las prácticas de seguridad de la información de los proveedores y la prestación de servicios.
A 5.23. Seguridad de la información para el uso de servicios en la nube	NUEVO	Los procesos de adquisición, uso, gestión y salida de los servicios en la nube se deben establecer, de acuerdo con los requisitos de seguridad de la información.

2.1.8.1. Seguridad de la información con proveedores para la gestión contractual

El Grupo de Contratos del Ministerio como parte de la gestión contractual:

- Coordina con las áreas los procesos de contratación para la adquisición del bien o servicio, fijando las especificaciones técnicas que debe cumplir los proveedores interesados en suministrar el bien y/o servicio, así como los recursos de personal, bienes, servicios e información que deben cumplir los acuerdos de nivel de servicio.
- Verifica que los procesos de contratación se adelanten acorde con los lineamientos de la ANCP y los proveedores se encuentren registrados en el sistema de información de Colombia Compra Eficiente -Secop, así mismo cumplan con los requisitos legales, económicos, de experiencia y técnicos para suministrar el bien o servicio.
- Asegura que los compromisos institucionales y las obligaciones contractuales estén claramente definidas en los contratos y se precise:
    - Las condiciones de confidencialidad de la información y protección de datos personales, el uso de bienes institucionales y la suscripción de Acuerdos de Confidencialidad con Contratistas o Proveedor para el desarrollo del objeto contractual y de los productos y servicios previstos.
    - La incorporación de los requisitos de seguridad y privacidad de la información, de gestión ambiental, de seguridad y salud en el trabajo y de calidad necesarios en el desarrollo del objeto contractual
- Designación del Supervisor o Interventor del contrato quien velara por la adecuada y oportuna ejecución del contrato y el recibo a satisfacción del bien o servicio contratado, así como de los activos que se suministren al proveedor y la información que se genere en desarrollo del objeto contractual.

2.1.8.2. Seguridad de la información con proveedores para recursos físicos

El Grupo Administrativa es el área encargada de la administración de la gestión de servicios generales, la seguridad y vigilancia de las áreas físicas, la administración de bienes muebles e inmuebles del Ministerio, del control de ingreso y salida de personal autorizado, vehículos y bienes. Los contratos de bienes y servicios para la gestión de recursos físicos establecen la suscripción de acuerdos de confidencialidad con contratistas y proveedores para la salvaguarda de áreas físicas de oficinas y restringidas o de información relacionada con la gestión de bienes inmuebles.

Articulación y coordinación con las Administraciones de las propiedades horizontales Edificio CCI y Palma Real para el ingreso y salida de personal autorizado, vehículos y bienes a través de los canales de comunicación definidos en los protocolos de seguridad para áreas comunes.

2.1.8.3. Seguridad de la información con proveedores para la gestión documental

El Grupo de Gestión Documental es responsable de la adquisición de bienes y servicios destinados para la administración, preservación y conservación de los registros documentales de archivos, así como de los servicios de transferencia de información por canales y medios electrónicos y del transporte documental de proveedores de mensajería, los contratos con los proveedores especifican los acuerdos de confidencialidad sobre la información y protección de datos personales, los acuerdos de nivel de servicios y las condiciones de entrega de los activos que transmiten o transportan los documentos institucionales.

2.1.8.4. Seguridad de la información con proveedores para la gestión tecnológica

La Oficina de Sistemas de Información es la responsable de la adquisición de bienes y servicios tecnológicos, y de la inclusión en los contratos de las obligaciones de confidencialidad sobre la información y protección de datos personales a la que tenga acceso los diferentes proveedores y contratistas o que sea generada en desarrollo del objeto contractual, así como suscribir los Acuerdos de Confidencialidad que aseguren el adecuado manejo de la información y bienes suministrados por la entidad requeridos por el proveedor o contratista y el cumplimiento de los acuerdos de nivel de servicios y las condiciones de entrega de los activos resultantes en desarrollo del objeto contractual.

2.1.8.5. Seguridad en la Cadena de Suministro de TIC

La Oficina de Sistemas de Información:

- Verifica la suscripción de Acuerdo de Confidencialidad de acuerdo con los niveles de acceso a los activos críticos tecnológicos y asegura que los ANS suscritos en los contratos se cumplan por parte

de los Proveedores en las condiciones pactadas para la entrega de los productos y servicios tecnológicos.
- Coordina con el Grupo Administrativa la entrada y salida de las instalaciones del Ministerio de productos – bienes tecnológicos – por parte del proveedor y se realice el registro de los bienes en el Inventario de Almacén.
- Coordina con los proveedores de servicios de comunicaciones, infraestructura, monitoreo y soporte técnico los accesos a la infraestructura tecnológica y áreas restringidas acorde con el desarrollo del objeto contractual.
- Coordina con los proveedores del desarrollo de aplicaciones y sitios web el acceso a los servidores en Centro de Computo o en la Infraestructura en Nube para el despliegue de las soluciones acorde con los requerimientos técnicos para la implementación de la solución.
- Coordina con el personal técnico de la oficina y los proveedores los cambios y actividades que desde el área tecnológica deben adelantarse para el despliegue de las soluciones o implementación de productos o servicios acorde con los requerimientos técnicos definidos para la implementación de la solución o producto, así como las pruebas de funcionalidad requeridos.

2.1.8.6. Uso de servicios en la nube

El Ministerio adquiere los servicios en la nube de acuerdo con la oferta detallada en el Acuerdo Marco de Colombia Compra Eficiente y las condiciones técnicas de los tipos de servicio de nube (IaaS, PaaS, SaaS) y servicios complementarios ofertados por los proveedores y requeridos por la entidad.
La Oficina de Sistemas de Información asegura que en el PETI se incorpore la implementación de capacidades de infraestructura en la nube para mejorar las condiciones técnicas de alojamiento de servidores, procesamiento y almacenamiento de información y se registre en el Plan Anual de Adquisiciones las necesidades específicas de adquisición del servicio de nube o de servicios en nube.

La Oficina de Sistemas de Información asegura que el servicio en nube cumpla con los requerimientos técnicos definidos y se entregue por parte del Proveedores de Servicios en Nube en los tiempos y capacidades adquiridos y las condiciones de seguridad de cómputo en la nube para el monitoreo de capacidades, tráfico y navegación de los servicios de aplicación y sitios web alojados en la nube por parte del servicio de monitoreo de plataforma tecnológica, lo que aplica a los servicios de aplicaciones web en nube para apoyar la gestión de la información en los procesos o servicios corporativos en nube.

2.1.9.Gestión de Incidentes de Seguridad y Privacidad de la Información

ISO/IEC 27001:2022 ANEXO A.1.	ISO/IEC 27001:2013 ANEXO A.	DESCRIPCIÓN ANEXO A.1.
A 5.24. Planificación y preparación de la gestión de incidentes de seguridad de la información	A.16.1.1. Responsabilidades y procedimientos	La organización debe planificar, uso, gestión y salida de los servicios en la nube, se deben establecer de acuerdo con los requisitos de seguridad de la información de la organización.
A 5.25. Evaluación y Decisión de Eventos de Seguridad de la Información	A.16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos	La organización debe evaluar los eventos de seguridad de la información y debe decidir, si clasificarlos como incidentes de seguridad de la información.
A 5.26. Respuesta a Incidentes de Seguridad de la Información	A.16.1.5. Respuesta a Incidentes de Seguridad de la Información	Los incidentes de seguridad de la información se deben responder de conformidad con los procedimientos documentados.
A 5.27. Aprender de los incidentes de seguridad de la información	A.16.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información	Los conocimientos adquiridos a partir de incidentes de seguridad de la información se deben utilizar para reforzar y mejorar los controles de seguridad de la información.
A 5.28. Recolección de Evidencia	A.16.1.7. Recolección de Evidencia	La organización debe establecer e implementar procedimientos para la identificación, recopilación, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información.

La Oficina de Sistemas de Información adelanta la gestión de incidentes de seguridad y privacidad de la información para dar respuesta oportuna a los eventos e incidentes detectados por los equipos de seguridad de perimetral y eventos reportados por capacidades de equipo, servicios de almacenamiento y uso de aplicaciones y sitios web. Los eventos e incidentes de seguridad y privacidad de la información se reportan en Mesa de Servicios al correo electrónico soportetecnico@mincit.gov.co y pueden ser registrados por:

- Los funcionarios, pasantes, contratistas, proveedores y partes interesadas ante cualquier situación, evento o escenario que evidencie amenaza o vulnerabilidad o riesgo materializado, en los servicios de aplicación o tecnológicos.
- Las amenazas reportadas por los equipos de seguridad perimetral son tratadas acorde con el procedimiento y guía para el análisis y gestión de eventos e Incidentes de Seguridad y Privacidad de la Información.
- Las alertas y boletines de vulnerabilidades o amenazas en internet informadas por Autoridades Cibernética.

2.1.9.1. Respuestas a Incidentes y Aprendizaje

La Oficina de Sistemas de información gestiona las capacidades operativa y técnicas para el manejo de incidentes que incluye la preparación, detección, análisis, contención, recuperación, respuesta a incidentes de seguridad en entornos On Premise y plataformas en la nube (IaaS, PaaS, SaaS).

Del análisis y resolución de incidentes de seguridad y privacidad de la información se establecen el mejoramiento de las políticas en equipos de seguridad, controles técnicos y operativos de la gestión tecnológica y aseguramiento de aplicaciones y sitios web.

2.1.10. Gestión de la Continuidad Tecnológica

ISO/IEC 27001:2022 ANEXO A.1.	ISO/IEC 27001:2013 ANEXO A.	DESCRIPCIÓN ANEXO A.1.
A 5.29. Seguridad de la información durante la interrupción.	A.17.1.1. Planificación de la continuidad de la seguridad de la información A.17.1.2. Implementación de la continuidad de la seguridad de la información A.17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debe establecer e implementar procedimientos para la identificación, recopilación, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información.

ISO/IEC 27001:2022 ANEXO A.1.	ISO/IEC 27001:2013 ANEXO A.	DESCRIPCIÓN ANEXO A.1.
A 5.30. Preparación de las TIC para la continuidad del negocio	NUEVO	La preparación para las TIC se debe planificar, implementar, mantener y probar basado en los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.

La continuidad de la gestión de TI se encuentra alineada con la continuidad del negocio del MinCIT y el cumplimiento de sus objetivos estratégicos.

La Oficina de Sistemas de Información para efectos de mantener la continuidad de los servicios de aplicación y servicios tecnológicos se aplica el procedimiento Gestión de la Continuidad de TI y la Guía DRP – Recuperación ante Desastres a fin de asegurar la disponibilidad de la plataforma tecnológica.

Los DRP documentados precisan los escenarios de recuperación de los servicios tecnológicos y controles implementados para mantener la disponibilidad de los servicios.

2.1.11. Cumplimiento de Requerimientos Normativos, Regulatorios y Auditoría

ISO/IEC 27001:2022 ANEXO A.1.	ISO/IEC 27001:2013 ANEXO A.	DESCRIPCIÓN ANEXO A.1.
A 5.31. Requisitos Legales, Reglamentarios y Contractuales.	A.18.1.1. Identificación de la legislación aplicable y de los requisitos contractuales A.18.1.5. Reglamentación de controles criptográficos	Los requisitos legales, reglamentarios y contractuales pertinentes para la seguridad de la información y el enfoque de la organización para cumplir estos requisitos se deben identificar, documentar y mantener actualizados.
A 5.32. Derechos de propiedad intelectual	A.18.1.2. Derechos de propiedad intelectual	La organización debe implementar procedimientos apropiados para proteger derechos de propiedad intelectual.
A 5.33. Protección de Registros	A.18.1.3. Protección de registros	Los registros deben estar protegidos contra pérdida, destrucción, falsificación, acceso y liberación no autorizada.
A 5.34. Privacidad y Protección de PII	A 8.1.4. Privacidad y protección de información de datos personales	La organización debe identificar y cumplir con los requisitos relacionados con la preservación de la privacidad y la protección de la PII de acuerdo con las leyes y regulaciones aplicables y los requisitos contractuales. PII (del inglés Personally Identifiable Information), Información Personal de Identificación
A 5.35. Revisión independiente de la seguridad de la información	A.18.2.1. Revisión independiente de la seguridad de la información	El enfoque de la organización para administrar la seguridad de la información y su implementación, incluida las personas, los procesos y las tecnológicas, se debe revisar de forma independiente a intervalos planificados o cuando ocurra cambios significativos.
A 5.36. Cumplimiento de Políticas, Normas y Estándares de Seguridad de la Información	A.18.2.2. Cumplimiento con las políticas y normas de seguridad A.18.2.3. Revisión del cumplimiento técnico	El cumplimiento de la política de seguridad de la información, el tema, las políticas específicas, las reglas y los estándares de la organización se debe revisar periódicamente.
A 5.37. Procedimientos operativos documentados	A 12.1.1. Procedimientos operativos documentados	Los procedimientos operativos de las instalaciones de procesamiento o la información se deben documentar y poner a disposición del personal que la necesite.

2.1.11.1. Requisitos y cumplimiento de obligaciones legales

El Ministerio da cumplimiento a las normas y regulaciones relacionadas con la seguridad y privacidad de la información y seguridad digital detalladas en el Normograma del Proceso Gestión de Tecnologías de la Información.

El alcance normativo se articula e implementa en:

- Procesos institucionales y en el entorno tecnológico.
- Se incorporan en los contratos y convenios mediante la suscripción de compromisos o acuerdos de confidencialidad sobre el manejo de la información y activos institucionales asociados.
- La adquisición de licencias de software con terceros o de software aplicativo con proveedores de desarrollado o desarrollos "in House".
- La regulación institucional en materia protección de datos.

2.1.11.2. Derechos de propiedad intelectual

El Ministerio da cumplimiento a las normas de propiedad intelectual emitidas por la Dirección Nacional de Derechos de Autor, relacionadas con los Derechos de Autor para el Uso de Software, material fílmico, fotográfico, de audio o de derechos conexos; e implementa los procedimientos, mecanismos y controles para garantizar el cumplimiento de las restricciones legales al uso del material protegido, mediante:
- La autorización de uso de material (documentos, fotografías, videos, audios) producidos como parte del ejercicio misional, o haciendo uso de material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordadas con los proveedores y conforme lo dispuesto por la normativa vigente.
- La documentación de licencias de software y de material documental producido o con autorización de uso por terceros.
- La instalación controlada en equipos institucionales de productos con licencia y licencias de software adquirido o con autorización de uso para la entidad.

2.1.11.3. Privacidad y protección de información de datos personales

El Ministerio en cumplimiento de las normas y regulaciones para la protección de los datos personales, regula el tratamiento de Datos Personales.

La socialización de la gestión de datos personales se presenta en el Comité Institucional de Gestión y Desempeño de acuerdo con la normatividad vigente y el procedimiento Gestión de Seguridad y Privacidad de la Información que incorpora el registro en el sistema de Información RNBD – Registro Nacional de Bases de Datos de la Superintendencia de Industria y Comercio.

2.1.11.4. Revisiones de seguridad y privacidad de la información

El MinCIT asegura el cumplimiento de las políticas de seguridad y privacidad de la información en sus procesos institucionales y de los procesos de revisión a la implementación y gestión en: los Comités Institucional de Gestión y Desempeño y de Control Interno; evaluación de los resultados de los procesos de auditoría de gestión, auditoría interna y/o auditoría independiente; resultados de evaluaciones de políticas FURAG – Formulario Único Reporte de Avances de la Gestión, Autodiagnósticos para la gestión de seguridad y privacidad de la información, la seguridad digital y la protección de datos.

2.1.11.5. Procedimientos operativos documentados

El proceso Gestión de Tecnologías de la Información incorpora los procedimientos y documentación estratégica para la gestión tecnológica, la seguridad de la información, gestión de ciberseguridad y continuidad tecnológica y de tratamiento de datos personales; así como los documentos de diagnóstico, revisión, evaluación y registro.

2.2. POLÍTICAS DE CONTROL DE PERSONAS

2.2.1.Seguridad del Recurso Humano

ISO/IEC 27001:2022 ANEXO A.1.	ISO/IEC 27001:2013 ANEXO A.	DESCRIPCIÓN ANEXO A.1.
A 6.1. Selección	A 7.1.1. Selección	Las verificaciones de los antecedentes de todos los candidatos para convertirse en personales deben llevar a cabo antes de unirse a la organización y de forma continúa teniendo en cuenta las leyes, regulaciones y ética aplicables y deben ser proporcionales a los requisitos comerciales, la clasificación de la información a la que se accederá y los riesgos percibidos.
A 6.2. Términos y condiciones de empleo	A 7.1.2. Términos y condiciones de empleo	Los acuerdos contractuales de empleo deben establecer las responsabilidades del personal y de la organización para la seguridad de la información.
A 6.3. Concientización, educación y capacitación en seguridad de la información	A 7.2.2. Toma de conciencia, educación y formación en la seguridad de la información.	El personal de la organización y las partes interesadas pertinentes deben recibir información, educación y capacitación adecuadas sobre seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, políticas y procedimientos específicos del tema, según sea pertinente para su función laboral.
A 6.4. Proceso Disciplinario	A 7.2.3. Proceso Disciplinario	Se debe formalizar y comunicar un proceso disciplinario para tomar medidas contra el personal y otras partes interesadas pertinentes que hayan cometido una violación de la política de seguridad de la información.
A 6.5. Responsabilidades después de la terminación o cambio de empleo	A.7.3.1. Terminación o cambio de responsabilidades de empleo	Las responsabilidades y los deberes de seguridad de la información que sigan siendo válidos después de la terminación o el cambio de empleo se deben definir, hacer cumplir y comunicar al personal pertinente y a otras partes interesadas.

2.2.1.1. Selección, Vinculación y Retiro

- **Selección y Vinculación**

En lo que corresponde a la gestión del personal de planta del Ministerio, el Grupo de Talento Humano aplica los lineamientos normativos y regulatorios vigentes.

En lo que respecta al personal contratista o proveedor el Grupo de Contratos en coordinación con las áreas que tiene bajo su cargo la función de supervisión, aplica los lineamientos normativos y legales para la contratación del personal requerido de acuerdo con las necesidades institucionales.

El personal del Ministerio sin importar su tipo de vinculación es responsable de la custodia y uso adecuado de los activos asignados en los que se incluyen: equipos (computadores, portátiles, medios de almacenamiento), datos e información, acceso a aplicativos y software, entre otros.
El personal del Ministerio deberá acoger las disposiciones de seguridad y privacidad de la información en este Manual.

- **Retiro de Personal**

Todo personal del Ministerio al momento de su retiro de la entidad, cambio de cargo o de área es responsable de entregar al Jefe inmediato o Supervisor del contrato los activos de información que se originen en desarrollo de sus funciones o actividad contratada.

Grupo Talento Humano Grupo de Contratos	• Informa a las áreas responsables de gestionar los activos de la Entidad, sobre el retiro, cambio de cargo o de área de los funcionarios, a fin de Inhabilitar o inactivar: los usuarios y contraseñas asignados para acceder a los servicios de TI y el carné de ingreso a las instalaciones físicas del Ministerio.
Jefes de área Supervisores de contratos	• Garantizan la retención de la información almacenada en los equipos (computador, portátil o tablets o en medios de almacenamiento externos) asignados al funcionarios, pasantes o contratistas, antes de su retiro formal de la entidad. • Garantizar la copia de seguridad de la información a cargo de funcionarios, pasantes o contratistas, en los medios de almacenamiento de la entidad durante y antes de la terminación del vínculo laboral con el Ministerio. • Garantizar la salvaguarda de la información física en condiciones de disponibilidad, integridad, privacidad y confiabilidad acorde con el proceso de Gestión Documental y los almacenamientos institucionales
Funcionarios Contratistas	• Hacer entrega al Grupo Administrativa de los bienes asignados para el desarrollo de las funciones o actividades contractuales y del carné para ingreso a las áreas del Ministerio acorde con los procedimientos relacionados con la Administración y Control de Bienes Devolutivos y de Consumo, Manejo Administrativo de los Bienes de Propiedad del Ministerio y los relacionados con los Controles físicos. • Hacer entrega al Grupo Gestión Documental de la información generada en el desarrollo de las funciones o actividades contractuales conforme los procedimientos de Gestión Documental.

2.2.1.2. Concientización en seguridad y privacidad de la información

Grupo Talento Humano	• Acorde con el procedimiento Vinculación y Retiro, desarrolla la Inducción y Re-Inducción a funcionarios, que incorporan los temas de Seguridad y Privacidad de la Información y Protección de Datos Personales. • Asegura que el Plan de Capacitación institucional, incorpore temáticas relacionadas con la seguridad de la información y protección de datos personales.
Oficina Sistemas de Información	• Asegura que la gestión de seguridad y privacidad de la información defina la estrategia de capacitación, comunicación y sensibilización y desarrolle temas de seguridad de la información, protección de datos personales, ciberseguridad y seguridad digital dirigida a todo el personal del Ministerio sin importar su tipo de vinculación.

	• Socializa a través de los medios de comunicación institucionales las alertas de seguridad y privacidad de la información y buenas prácticas para el manejo de los activos de información y datos personales.
Oficina Asesora de Planeación Sectorial	• Asegura que los temas relacionados con las Políticas de Gobierno y Seguridad Digital se integren en el Modelo Institucional de Operación. • Garantiza que el Comité Institucional de Gestión y Desempeño se informe sobre la implementación, mantenimiento, seguimiento y evaluación de las Políticas de Gobierno y Seguridad Digital y la protección de datos personales.

2.2.1.3. Procesos disciplinarios

Juzgamiento Disciplinario	• Adelanta la gestión disciplinaria y el procedimiento Acciones Disciplinarias conforme a la normatividad vigente y desarrolla la investigación preliminar disciplinaria de los procesos bajo la clasificación de reserva, asegurando los controles de seguridad y privacidad para la información; así mismo comunica y socializa los aspectos de la gestión disciplinaria y su aplicación de interés y aplicación general.
Grupo de Contratos	• Verifica el cumplimiento de las obligaciones contractuales, en los casos de incumplimiento y realización de calidad de los bienes y servicios, adelantando en coordinación con la Oficina Asesora Jurídica la revisión del incumplimiento y determinando las acciones para determinar el incumplimiento o de conciliación.
Supervisores	• Verifica el cumplimiento contractual e informa al Grupo de Contratos el incumplimiento a fin de que se adelante la gestión para declarar el incumplimiento y de conciliación si es del caso.

2.2.2. Acuerdos de Confidencialidad

ISO/IEC 27001:2022 ANEXO A.1.	ISO/IEC 27001:2013 ANEXO A.	DESCRIPCIÓN ANEXO A.1.
A 6.6. Acuerdos de confidencialidad o no divulgación	13.2.4. Acuerdos de confidencialidad o no divulgación	Los acuerdos de confidencialidad o no divulgación que reflejenlas necesidades de la organización para la protección de la información deben ser identificados, documentados, revisados y firmados periódicamente por el personal y otras partes interesadas pertinentes.

La gestión contractual asegura que los compromisos institucionales y las obligaciones contractuales estén claramente definidas en los contratos y precisa:

- Las condiciones de confidencialidad de la información y protección de datos personales, el uso de bienes institucionales y la suscripción de Acuerdos de Confidencialidad con Contratistas o Proveedor para el desarrollo del objeto contractual y de los productos y servicios previstos.
- La incorporación de los requisitos de seguridad y privacidad de la información, de gestión ambiental, de seguridad y salud en el trabajo y de calidad necesarios en el desarrollo del objeto contractual.

La Supervisión de contratos acorde con la criticidad de los activos asignados para la ejecución del objeto contractual y el desarrollo de los productos y servicios garantizando la protección de la información.

2.2.3.Teletrabajo y trabajo remoto

ISO/IEC 27001:2022 ANEXO A.1.	ISO/IEC 27001:2013 ANEXO A.	DESCRIPCIÓN ANEXO A.1.
A 6.7. Trabajo Remoto	A 6.2.2 Trabajo Remoto	Las medidas de seguridad se deben implementar cuando el personal trabaje de forma remota para proteger la información a la que se accede, procesa o almacena fuera de las instalaciones de la organización.

2.2.3.1. Teletrabajo

Grupo de Talento Humano	El Teletrabajo está reglamentado en el Ministerio, establece el procedimiento para la implementación del trabajo en modalidad suplementario, requerimientos para el teletrabajo y tiempo de duración, y compromisos de seguridad y privacidad de la información y protección de datos personales.
Oficina de Sistemas de Información	Establece las condiciones y requisitos para el establecimiento de conexiones remotas a la plataforma tecnológica de la Entidad; así mismo, suministra las conexiones y se realicen de manera segura y verifica que los equipos de cómputo asignado cuenten con los programas de escritorio, antivirus y antimalware y forma parte del Plan de Mantenimiento de Equipos de Usuario Final.
Funcionarios	- Deben hacer uso adecuado y exclusivo de los recursos tecnológicos asignados (computador, tablets, portátil u otros) para el cumplimiento de las funciones asignadas en teletrabajo y facilitar el equipo para el mantenimiento preventivo o correctivo programado. - Deben asegurarse de mantener la debida integridad, confidencialidad y disponibilidad de la información, así como de la privacidad de los datos personales objeto del desarrollo de sus funciones. - Reportar en la Mesa de Servicios(soportetecnico@mincit.gov.co) cualquier evento relacionado con la funcionalidad de los recursos tecnológicos asignados. - Abstenerse de instalar software o programas ejecutables en los equipos asignados sin previa autorización de la Oficina de Sistemas de Información, quien verificará la necesidad y las implicaciones de seguridad de su instalación.

2.2.3.2. Trabajo con Acceso Remoto

Para la realización de trabajo con acceso remoto por parte de funcionarios o personal contratista o proveedor está disponible el acceso a los servicios de aplicación a través del sitio web institucional www.mincit.gov.co – Ministerio – Mintranet, con acceso mediante autenticación de doble factor. El acceso a través de VPN debe estar autorizado por el Jefe del área del funcionario o del Supervisor del contratista o proveedor al servicio de aplicación o sitio web, o equipos de la infraestructura acorde con la función o actividad en desarrollo del objeto contractual.

2.2.3.3. Eventos de seguridad de la información

ISO/IEC 27001:2022 ANEXO A.1.	ISO/IEC 27001:2013 ANEXO A.	DESCRIPCIÓN ANEXO A.1.
A 6.8. Informes de eventos de seguridad de la información	A 16.1.2. Reporte de eventos de seguridad de la información A 16.1.3. Reporte de debilidades de seguridad de la información	La organización debe proporcionar un mecanismo para que el personal informe oportunamente sobre los eventos de seguridad de la información observados o sospechosos a través de los canales apropiados.

La Oficina de Sistemas de Información es la encargada de implementar los controles de seguridad informática, ciberseguridad y seguridad digital en el Ministerio.

- **Equipos de cómputo institucionales**

Todos los servidores, computadores y portátiles del Ministerio cuenten con la instalación y actualización del software de antivirus - antimalware, con actualización en línea y la actualización de firmas, así mismo se encuentren monitoreados por los equipos de seguridad.

- **Monitoreo para la ciberseguridad y seguridad digital**

La plataforma de monitoreo permite contar con la información relacionada con la protección del correo electrónico, navegación en Internet y monitoreo antimalware basado en el comportamiento de usuarios, aplicaciones y sitios web, detectar vulnerabilidades y reportar alertas de seguridad informática sobre las capacidades de los recursos de la infraestructura amenazas, e incidentes de seguridad de la información.

- **Respuesta a eventos e incidentes**

Contar con la información de alertas y logs para realizar el análisis de los eventos e incidentes de seguridad y privacidad de la información y determinar las acciones de remediación a las vulnerabilidades detectas, e implementar o mejorar las políticas en equipos de seguridad, controles técnicos y operativos de la gestión tecnológica y aseguramiento de servidores, perfiles de usuario, aplicaciones y sitios web.

- **Detección de vulnerabilidades**

Las pruebas de vulnerabilidad e intrusión permiten determinar los activos vulnerables y determinar las acciones de remediación respectivas, así como coordinar con proveedores su implementación acorde con el alcance de la remediación.

2.3. POLÍTICAS DE CONTROL FÍSICO

2.3.1.Seguridad Física y del Entorno

ISO/IEC 27001:2022 ANEXO A.1.	ISO/IEC 27001:2013 ANEXO A.	DESCRIPCION ANEXO A.1.
A 7.1. Perímetros de Seguridad Física	A 11.1.1. Perímetros de Seguridad Física	Los perímetros de seguridad se deben definir y utilizar para proteger las zonas que contengan información y otros activos asociados.
A 7.2. Entrada física	A 11.1.2. Controles físicos de entrada A 11.1.6. Áreas de despacho y carga	Las zonas seguras deben estar protegidas por controles de entrada y puntos de acceso adecuados.
A 7.3. Asegurar Oficinas, Habitaciones e Instalaciones (*Aseguramiento de Oficinas, Salas e Instalaciones)*	A 11.1.3. Seguridad de oficinas, recintos e instalaciones	Se debe diseñar e implementar la seguridad física de las oficinas, salas e instalaciones
A 7.4. Monitoreo de seguridad física	NUEVO	Las instalaciones deben ser monitoreadas continuamente para detectar accesos físicos no autorizados.
A 7.5. Protección contra amenazas físicas y ambientales	A 11.1.4. Protección contra amenazas externas y ambientales	Se debe diseñar e implementar la protección contra las amenazas físicas y medioambientales, como las catástrofes naturales y otras amenazas físicas intencionadas o no intencionadas a las infraestructuras.
A 7.6. Trabajar en áreas seguras	A 11.1.5. Trabajo en áreas seguras	Se debe diseñar e implementar medidas de seguridad para trabajar en zonas seguras.

2.3.1.1. Acceso Físico y Autenticación personal

El Ministerio cuenta con los mecanismos de control de acceso físico y de autenticación para el personal funcional, contratista o de proveedores coordinado entre el área respectiva y el Grupo Administrativa con la Administración de las copropiedades donde la entidad tiene sus oficinas, bodegas, parqueaderos y áreas restringidas, así como de los bienes de propiedad o en custodia de la entidad.

2.3.1.2. Áreas Seguras

El Ministerio garantiza la implementación de controles de seguridad física e informática para la protección de las instalaciones de procesamiento de información y cualquier otra área considerada crítica para la operación de la Entidad.

El Grupo Administrativa asegura que los usuarios del Ministerio - funcionarios, pasantes, contratistas, proveedores y ciudadanía- cuenten con:

- La identificación institucional o permiso de acceso previamente autorizado para el ingreso físico de la persona, vehículo o bien a las áreas autorizadas.
- El registro de ingreso temporal o permanente al área específica de la personal en los puntos de control o recepción a el área, con el registro de ingreso o retiro de objetos personales, de equipos de cómputo o de cualquier otro bien de propiedad de la entidad o que se encuentre dentro de las instalaciones de la entidad.
- Coordinar con las administraciones de las copropiedades el respectivo monitoreo en áreas comunes y registro del monitoreo de video vigilancia en las áreas institucionales.

2.3.1.3. Seguridad Física y Ambiental

- **Grupo Administrativa**

Asegura que en las instalaciones del Ministerio - oficinas, bodegas, parqueaderos y áreas restringidas, así como de los bienes de propiedad o en custodia de la entidad – se implementen los controles de seguridad relacionados con:

- La Video Vigilancia y la respectiva comunicación a personal del ministerio y visitantes del cumplimiento de la protección de datos personales.
- Sistema contra incendios para prevención de eventos de conflagración y señalización para la ubicación de extintores, mangueras y alarmas de emergencia, áreas de evacuación y coordinación de crisis con las copropiedades, entidades de emergencia y de seguridad nacional.
- Evaluación y manejo de sustancias peligrosas en áreas sociales y restringidas.
- Ingreso y retiro de bienes propios o en custodia, material desechable o de reciclaje acorde con los protocolos de ingreso y salida de las copropiedades.

- **Grupo Talento Humana**

Asegura la implementación del Sistema de Riesgos Laborales para la protección de la integridad del personal del Ministerio y de los controles para la identificación de prácticas, procesos, situaciones peligrosas y de acciones de intervención de riesgos propios del entorno institucional y del entorno de la entidad.

2.3.2. Escritorio y Pantalla Limpia

ISO/IEC 27001:2022 ANEXO A.1.	ISO/IEC 27001:2013 ANEXO A.	DESCRIPCIÓN ANEXO A.1.
A 7.7. Limpiar escritorio y limpiar pantalla	A 11.2.9. Política de escritorio y pantalla limpios	Se deben definir e implementar adecuadamente normas claras para los papeles y los soportes de almacenamiento extraíbles y normas claras sobre pantallas claras para las instalaciones de tratamiento de la información.

El Ministerio promueve:

- La política de escritorio limpio en los lugares de trabajo y áreas seguras para proteger la información crítica o sensible en medios impresos y digitales, en archivos de gestión y medios de almacenamiento externos requeridos por los procesos.

- La política de pantalla limpia en computadores, portátiles y servidores, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

Los funcionarios, pasantes, contratistas, proveedores o partes interesadas deben tener en cuenta las siguientes consideraciones para la protección de activos de propiedad del Ministerio:
- En los lugares de trabajo solo deben permanecer los documentos y elementos necesarios para la realización de las labores. No se deben dejar documentos originales, preliminares o finales con información reservada o clasificada a la vista de otras personas, o desatendidos en otro lugar diferente al sitio de trabajo. Las copias de trabajo deben ser destruidos antes de ser arrojados a la basura. No se deben reutilizar documentos impresos que contengan información reservada o clasificada.

- Se debe aplicar los controles de seguridad y privacidad de la información para los activos sensibles y críticos determinados por el Ministerio con el fin de salvaguardar la información reservada o clasificada que se encuentre en cualquier medio.

- La liberación de los trabajos de impresión o de escáner de documentos se realizará a través de autenticación cumpliendo con los requerimientos de disponibilidad, confidencialidad y cero desperdicios de papel.

2.3.3. Protección y Seguridad de Activos

ISO/IEC 27001:2022 ANEXO A.1.	ISO/IEC 27001:2013 ANEXO A.	DESCRIPCIÓN ANEXO A.1.
A 7.8. Ubicación y protección de equipos	A 11.2.1. Ubicación y protección de los equipos	Emplazamiento y protección en equipos.
A 7.9. Seguridad de activos fuera de las instalaciones	A 11.2.6. Seguridad de equipos y activos fuera de las instalaciones.	Los activos externos deben estar protegidos.
A 7.10. Medios de almacenamiento	A 8.3.1. Gestión de medios removibles A 8.3.2. Disposición de los medios A 8.3.3. Transferencia de medios físicos A 11.2.5. Retiro de activos	Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y disposición de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.
A 7.11. Servicios Públicos de apoyo (*Utilidades de apoyo)*	A 11.2.2. Servicios de suministro	Las instalaciones de procesamiento de la información deben estar protegidas contra los cortes de energía y otras interrupciones causadas por fallos en los servicios públicos de apoyo.

2.3.3.1. Dispositivos móviles

El uso de dispositivos móviles portátiles, tablets, celulares, entre otros, de propiedad el Ministerio o de personal o visitantes de la entidad:

- Aplica controles físicos, acorde con los lineamientos y directrices para la Administración y Control de Bienes Devolutivos y de Consumo, y registro de control de ingreso y retiro físico de equipos o bienes tecnológicos.

- Aplica controles lógicos para el acceso a la red institucional y servicios de TI por parte de funcionarios, personal y visitantes; el monitoreo de navegación de usuarios, equipos (IPs, MACs); generación de copias de seguridad periódica, entre otros.

2.3.3.2. Manejo de la información en medios físicos y electrónicos

El Ministerio como propietario y custodio de la información (física o electrónica) generada como resultado de la gestión y acorde con la normatividad que le sea aplicable para la gestión documental institucional, se reserva el derecho de su conservación o destrucción, dependiendo del nivel de criticidad definida para la información con base en los lineamientos del Archivo General de la Nación y del Comité Institucional de Gestión y Desempeño en lo referente a la Gestión Documental.

Los funcionarios y/o contratistas a quienes se les asignen medios removibles institucionales deben tomar las medidas para el almacenamiento y resguardo de la información y realizar respaldo de esta en los medios de almacenamiento en nube asignados, evitando accesos no autorizados, pérdida de información o extravío del medio.

Todo medio de almacenamiento removible es escaneado por la solución antivirus/antimalware institucional cada vez que sea conectado a la red interna.

Los medios de almacenamiento removibles no son una alternativa individual de respaldo de información, siendo responsabilidad de los usuarios llevar la información de estos medios a los almacenamientos en nube o servidores de datos para mantener su disponibilidad, confidencialidad e integridad.

2.3.3.3. Uso y manejo de medios almacenamiento removibles

La información institucional crítica o sensible almacenada en un medio removible (Discos Duros, CDs, Discos Ópticos) con un tiempo de retención definida por el Grupo de Gestión Documental y acorde con el Programa de Conservación y Preservación aplica los lineamientos definidos para la transferencia o respaldo en otro medio para evitar la pérdida de información.

En caso de requerirse almacenar información crítica o sensible en medios de almacenamiento removibles, esta solo será almacenada en medios dispuestos por la entidad de acuerdo con los lineamientos para la Administración y Control de Bienes Devolutivos y de Consumo, y deberán implementar una técnica de cifrado para salvaguardar su integridad y confiabilidad.

La información en medio de almacenamiento removibles deberá alinearse con lo definido en la TRV – Tabla de Valoración Documental y TRD -Tabla de Retención del área propietaria e la información.

2.3.3.4. Uso y manejo de medios almacenamiento en nube

Todo el personal del Ministerio sin importar su tipo de vinculación debe hacer uso de los medios de almacenamiento en nube y servidores de datos disponibles por la Entidad, para salvaguardar la información institucional generada en desarrollo de las actividades funcionales y obligaciones contractuales, con el fin de facilitar la disponibilidad a la misma. Es responsabilidad de los usuarios mantener la información en los almacenamientos asignados.

Es responsabilidad de funcionarios y Supervisores de Contratos tomar las medidas adecuadas para el almacenamiento y resguardo de la información en los medios de almacenamiento en nube asignados, evitando accesos no autorizados, pérdida de información o extravío del medio.

2.3.3.5. Suministro de Servicios Públicos

Las instalaciones físicas donde se encuentran las oficinas y diferentes áreas del Ministerio en coordinación con las copropiedades se articula con los protocolos para tender emergencias y suspensión de servicios públicos básicos - luz, agua, gas, teléfonos – que respaldan el funcionamiento temporal ente el evento que surja y permita la oportuna implementación del Plan de Emergencias Institucional para la salvaguarda de la vida del personal de la Entidad y mantener la continuidad de los servicios de operación y tecnológicos institucionales.

2.3.4. Protección y Seguridad de la Red y Equipos

ISO/IEC 27001:2022 ANEXO A.1.	ISO/IEC 27001:2013 ANEXO A.	DESCRIPCIÓN ANEXO A.1.
A 7.12. Seguridad del cableado	A 11.2.3. Seguridad del cableado	Los cables que transportan energía, datos o servicios de información de apoyo deben estar protegidos contra la interceptación, las interferencias o los daños.
A 7.13. Mantenimiento de equipo	A 11.2.4. Mantenimiento de equipos	El equipo se debe mantener correctamente para asegurar la disponibilidad, integridad y confidencialidad de la información.
A 7.14. Eliminación segura o reutilización de equipos	A 11.2.7. Disposición segura o reutilización de equipos	Los elementos de los equipos que contengan medios de almacenamiento se deben verificar para asegurarse de que los datos sensibles y el software con licencia se han eliminado o sobrescrito de forma segura antes de su disposición o reutilización.

2.3.4.1. Controles de redes y seguridad de los servicios de red

En el Ministerio la Oficina de Sistemas de Información administra la red de telecomunicaciones y demás equipos y dispositivos conectados a la red y coordina la implementación de servicios tecnológicos que se incorporen a la infraestructura tecnológica, el acceso de contratistas y

proveedores a recursos de acuerdo con el alcance de la actividad a realizar mantenimiento preventivo o correctivo o cambios en las plataformas de aíres acondicionados, planta eléctrica, mantenimientos de equipos.

2.3.4.2. Mantenimiento preventivo y correctivo de equipos

El Ministerio asegura a través de la Oficina de Sistemas de Información se implemente el Plan de Mantenimiento a Equipos y Servicios Tecnológicos, así como se cumpla con los lineamientos ambientales para el manejo y disposición final de equipos, partes y sustancias o elementos contaminantes.

La disposición final de equipos institucionales - servidores, PCs, portátiles, discos duros deberán pasar por el proceso de formateo físico y/o lógico antes de su devolución al Grupo de Almacén para su reasignación o baja del inventario.

2.3.4.3. Aseguramiento y reutilización de equipos

- **Aseguramiento**

En el Ministerio cuenta con controles que le permiten monitorear la disponibilidad e integridad de la infraestructura tecnológica, así como los niveles adecuados de mantenimiento y soporte a la infraestructura de red, plataformas operativas, sistemas de información, aplicativos y sitios web, hardening de servidores, entre otros.

- **Pérdida o robo del dispositivo móvil de propiedad del Ministerio**

El responsable del dispositivo debe reportar de manera inmediata el hecho al Jefe inmediato, Grupo Administrativa y Grupo de Ingeniería y Soporte Técnico, a fin de realizar las siguientes acciones:
- Registrar la denuncia de pérdida del bien institucional en el Portal CSIRT Policía Nacional.
- Inhabilitar/bloquear accesos al usuario y servicios asociados como VPN, entre otros.
- Reactivar usuario y gestionar nueva contraseña.
- Adelantar con la aseguradora el trámite de recuperación del bien.
- Asignación de nuevo equipo acorde con los lineamientos de la Administración y Control de Bienes Devolutivos y de Consumo.

2.4. POLÍTICAS DE CONTROL TECNOLÓGICO

2.4.1. Dispositivos de Usuario Final

ISO/IEC 27001:2022 ANEXO A.1.	ISO/IEC 27001:2013 ANEXO A.	DESCRIPCIÓN ANEXO A.1.
A 8.1. Dispositivos de punto final de usuario	A 6.2.1. Política para dispositivos móviles A 11.2.8. Equipos de usuario desatendido	Se debe proteger la información almacenada, procesada o accesible a través de los dispositivos de punto final del usuario

2.4.1.1. Dispositivos Institucionales de Usuario Final

El Ministerio a través del Grupo Administrativa controla la asignación y devolución de equipos - PC o portátil y/o medios de almacenamiento removibles – asignados a funcionarios para el desarrollo de sus funciones y contratistas para el desarrollo de su objeto contractual, para este último el Supervisor verifica que al finalizar el contrato se realice la devolución de los bienes asignados.

Todos los dispositivos institucionales están debidamente identificados con el fin de controlar el acceso físico a instalaciones y acceso lógico mediante autenticación con usuario y contraseña asignados, son atendidos por el servicio de soporte técnico y forman parte de los programas de mantenimiento preventivo y correctivo periódicos.

Todo equipo que se conecte a la red institucional es monitoreado por los equipos de la plataforma de seguridad digital de la entidad, las alertas o incidentes que se presenten como resultado de acceso a servicios tecnológicos, aplicaciones y sitios web autorizados serán tratados conforme a los procedimientos de Gestión de Incidentes de Seguridad y Privacidad de la Información, Operación de la Gestión Tecnológica y Gestión de Cambios implementados por el Proceso de Gestión Tecnológica.

2.4.1.2. Dispositivos No Institucionales

Para funcionarios y contratistas que se conecten a la red institucional con equipos no institucionales, serán monitoreados desde el momento de su
autenticación mediante usuario y contraseña, así como el acceso a los servicios tecnológicos corporativos, aplicaciones y sitios web institucionales a los que el usuario se le haya concedido acceso.

El servicio de soporte técnico solo atenderá casos relacionados con la gestión de accesos otorgados a los servicios tecnológicos, aplicaciones y sitios web institucionales.

Los equipos no institucionales no forman parte de los programas de mantenimiento preventivo y correctivo a equipos institucionales, por lo tanto, el dueño del equipo no institucional es responsable de la seguridad física e informática (licencias de software de escritorio, virus y antimalware) y del mantenimiento preventivo o correctivo que requiera el equipo.

2.4.1.3. Equipos institucionales fuera de las instalaciones

Los funcionarios que desarrollan sus funciones en modalidad de teletrabajo - trabajo suplementario y contratistas en modalidad de trabajo remoto con equipos institucionales, son responsables y custodios del bien asignado, así como de la información que se encuentre almacenada en el dispositivo, para lo cual deben tener en cuenta que el Ministerio asigna los equipos institucionales portátiles con guaya de seguridad, por lo tanto, deben anclar estos equipos al punto de trabajo, estos equipos no deben ser manipulados por personas diferentes a los responsables.

La Oficina de Sistemas de Información como parte del plan de mantenimiento preventivo o correctivo o de la actualización tecnológica los equipos institucionales, los cuales deben ser entregados acorde con las instrucciones que se impartan para el efecto.

En caso de pérdida o robo del equipo de propiedad del Ministerio deberá aplicarse lo definido en el ítem 2.3.4.4. Aseguramiento y reutilización de equipos.

2.4.1.4. Acceso a la información y Activos Tecnológicos

ISO/IEC 27001:2022 ANEXO A.1.	ISO/IEC 27001:2013 ANEXO A.	DESCRIPCIÓN ANEXO A.1.
A 8.2. Derechos de acceso privilegiado	A 9.2.3. Gestión de derechos de acceso privilegiado	La asignación y el uso de los derechos de acceso privilegiado deben estar restringidos y gestionados.
A 8.3. Restricción de acceso a la información	A 9.4.1. Restricción de acceso a la información	El acceso a la información y a otros activos asociados se debe restringir de acuerdo con la política específica establecida sobre el control de acceso.
A 8.4. Acceso al código fuente	A 9.4.5. Control de acceso a códigos fuente de programas	El acceso para leer o escribir sobre un código fuente, las herramientas de desarrollo, y las librerías de software se deben gestionar apropiadamente.
A 8.5. Autenticación segura	A 9.4.2. Procedimiento de ingreso seguro	Se deben implementar tecnología y procedimientos de autenticación seguros basados en restricciones de acceso a la información y en la política específica del tema sobre el control de acceso.

2.4.1.5. Acceso a servicios tecnológicos transversales

El personal del Ministerio sin importar su vinculación una vez conectados a la red institucional tienen acceso a los servicios tecnológicos como correo electrónico, internet o aplicaciones internas, almacenamiento en nube y servidores de datos.

Los funcionarios, contratistas y proveedores de servicios encargados de administrar la infraestructura tecnológica cuentan con los permisos de acceso, debidamente autorizados por la Oficina de Sistemas de Información, a consolas de administración, servidores, equipos de red y áreas restringidas acorde con el perfil asignado y alcance de la actividad a realizar.

La Oficina de Sistemas de Información establece los requisitos para el establecimiento de conexiones remotas a la plataforma tecnológica de la Entidad; así mismo, implementa los controles necesarios para que tales conexiones se realicen de manera segura.

Los funcionarios, contratistas o proveedores del Ministerio, que en razón a sus labores requiera tener acceso a los componentes de la infraestructura tecnológica y a los repositorios de la información institucional:

• De manera física deberán contar con la autorización ingreso al área restringida de la Oficina de Sistemas de Información y autorización de ingreso a las instalaciones de la entidad del Grupo Administrativa.
• Desde redes externas, deben acceder remotamente mediante conexiones seguras (https, VPN) aplicando el proceso de autenticación acorde con el componente o servicio específico, previamente autorizado por su Jefe inmediato e informada la Oficina de Sistemas de Información.

2.4.1.6. Uso de recursos tecnológicos corporativos

Los recursos tecnológicos corporativos son herramientas de trabajo esenciales para las labores diarias, por lo tanto, funcionarios, pasantes, contratistas, proveedores, visitantes y demás partes interesadas con acceso a la red institucional deben hacer uso adecuado de estos.
Los recursos tecnológicos corporativos son plataformas en nube o institucionales las cuales son de acceso transversal a toda la Entidad y son de acceso para todo el personal del Ministerio sin importar su vinculación a través del usuario y contraseñas asignadas, y para algunos servicios de aplicación o sitios web con el usuario y contraseña específica.

El Ministerio controla, verifica y monitorea el uso adecuado de los servicios: de internet; las plataformas corporativas - almacenamiento en nube, correo electrónico, Teams, y demás aplicaciones en línea-; aplicaciones y sitios web como la Mintranet; servicio de impresión, entre otros recursos tecnológicos.
Consideraciones generales para el uso de internet, plataformas corporativas, aplicaciones y sitios web, servicios y recursos tecnológicos por parte del personal del Ministerio independiente de su vinculación:
• Únicamente pueden ser utilizada para finalidades relacionadas con el desarrollo de las funciones correspondientes al cargo o función, u obligaciones definidas en el respectivo contrato, quedando limitado el uso al ámbito laboral institucional.
• Los accesos a estos recursos son personales e intransferibles.
• En caso de retiro de los funcionarios, pasantes, contratistas, proveedores, visitantes u otras partes interesadas, debe ser informada la Oficina de Sistemas de Información a fin de retirar/inhabilitar/bloquear el acceso otorgado.
• En caso de ausencia temporal de funcionarios y contratistas estos deben establecer en el servicio de correo electrónico la redirección de mensajes; e informar a la Oficina de Sistemas de

Información que se inhabiliten/bloqueen los usuarios en servicios como VPN, administración de componentes tecnológicos o su cuenta de usuario institucional.
• Cualquier correo electrónico sospechoso debe ser reportado a soportetecnico@mincit.gov.co.
• Los funcionarios o contratistas que tengan atribuida la gestión de cuentas de correo genéricas asociadas a la recepción de trámites, atención de servicios o asociadas a servicios de aplicación y sitios web, o recursos tecnológicos no podrán en ningún caso hacer uso de ellas por motivos personales o para la gestión laboral institucional diferente al alcance definido para tales cuentas de correo.
• Toda la información almacenada, gestionada o transmitida a través de las plataformas corporativas - almacenamiento en nube, correo electrónico, Teams, y demás aplicaciones en línea- ; aplicaciones y sitios web como la Mintranet; servicio de impresión, entre otros recursos tecnológicos es propiedad del Ministerio.
• Cuando se realice el envío de información pública reservada o publica clasificada mediante correo electrónico, se aplicarán Acuerdos de Confidencialidad definidos entre las partes y los mecanismos que salvaguarden la autenticidad e integridad de la información.
• Las plataformas corporativas; aplicaciones y sitios web, entre otros recursos tecnológicos es propiedad del Ministerio no deben ser utilizados para enviar ni recibir información diferente a la relacionada con la gestión institucional, ni contestar mensajes o cadenas de mensajes que no se encuentren implementados como parte de la comunicación interna institucional, ni ser utilizados para guardar información personal, ni registrar en plataformas web externas la cuenta de usuario institucional sin autorización del Jefe Inmediato y verificación de seguridad del sitio o plataforma web por parte de la Oficina de Sistemas de Información.

2.4.1.7. Internet

El servicio de internet institucional se dispone para la conexión de los usuarios de los servicios tecnológicos, plataformas corporativas, aplicaciones y sitios web, por parte del personal del Ministerio y ciudadanos.

Los sitios web del Ministerio están diseñados para publicar la información de la gestión institucional, por tanto, el personal responsable de administrar o publicar contenidos en los sitios web, deberán cumplir con los requerimientos normativos y regulatorios relacionados con Transparencia y Acceso a la Información Pública; así mismo, no podrán publicar información diferente a la específica del sitio web, ni información personal o de otra índole.

El personal del Ministerio sin importar su tipo de vinculación que acceden a internet con usuario y contraseña institucional, no cuentan con permisos de navegación en internet a:

• Sitios web relacionados con actividades de juego o apuestas;
• Sitios web de contenido para adultos relacionados con pornografía, pedofilia o erotismo, o cualquier otro dentro de la misma categoría.

• Sitios web de carácter discriminatorio, racista, o material potencialmente ofensivo, menosprecio o acoso explícito.
• Sitios web que puedan afectar la seguridad informática, los cuales puedan poner en riesgo la disponibilidad de los servicios tecnológicos, integridad y confidencialidad de la información institucional.
• Sitios de descarga de material protegido bajo leyes de derecho de propiedad sin que se cuente con la autorización expresa o licencia de uso respectiva, o archivos electrónicos para usos no relacionados con la misionalidad del Ministerio.
• Sitios web que inciten a la participación en cualquier actividad ilegal o criminal.
El Ministerio monitorea la navegación hacia y desde internet de sus usuarios institucionales, aplicaciones y sitios web, de los servicios de conexión remota (VPN) y demás servicios tecnológicos; bloquea la navegación a sitios web sospechosos o categorizados como peligrosos; bloque la transferencia o transmisión de información anómala o no autorizada.
El personal del ministerio que como parte del desarrollo de las labores institucionales requiera el acceso a un sitio web específico al que no esté permitida su navegación, deberá previamente justificar la necesidad de acceso al sitio o plataforma web externa y obtener la autorización formalizada por parte de su jefe inmediato o supervisor del contrato, y solicitar a la Oficina de Sistemas de Información la habilitación del acceso al sitio web especificado por tiempo limitado, así mismo se realizará el monitoreo de la navegación que se realice hacia o desde el sitio web autorizado.

2.4.1.8. Control y acceso a código fuente, programas y licencias

El Ministerio cuenta con los controles operativos e informáticos para la gestión de licencias de herramientas de desarrollo, Bibliotecas de software y código fuente de las aplicaciones y sitios web, software utilitario, y licencias de software operativo, de uso y ejecución, entre otros.
La Oficina de Sistema de Información administra la instalación y configuración en servidores de bases de datos y aplicaciones y sitios web en ambientes de desarrollo y producción, servidores de almacenamiento de datos, de dispositivos y equipos de usuario final de las licencias de software requeridas para el desarrollo y uso de aplicaciones y sitios web, implementación de servicios tecnológicos y plataformas corporativas.

El acceso a servidores en la infraestructura tecnológica institucional por parte de funcionarios, contratistas y proveedores de desarrollos acceden mediante VPN y acceso con usuario y contraseña al dispositivo específico.

Se implementa la política de copias de seguridad y Backup de los servidores de los programas fuentes de desarrollos propietarios institucionales y de los ejecutables de los desarrollos de software con proveedores.

2.4.2. Gestión de la capacidad tecnológica

ISO/IEC 27001:2022 ANEXO A.1.	ISO/IEC 27001:2013 ANEXO A.	DESCRIPCIÓN ANEXO A.1.
A 8.6. Gestión de capacidad	A 12.1.3. Gestión de capacidad	El uso de los recursos se debe monitorear y ajustar en función de las necesidades de capacidades actuales y previstas.

El Ministerio garantiza la disponibilidad de los recursos tecnológicos institucionales, para el efecto la Oficina de Sistemas de Información:

• Monitorea las capacidades de los servicios tecnológicos, servidores de aplicación y bases de datos, canales de internet, almacenamientos, y el mantenimiento preventivo y correctivo de componentes tecnológicos y de usuario, plataformas de aíres acondicionados, planta eléctrica, entre otros.
• Identifica las necesidades a nivel tecnológico, con el fin de evitar potenciales indisponibilidades de los servicios de tecnológicos y de aplicación y sitios web, para mantener la continuidad ante los cambios en la infraestructura tecnológica.

2.4.3. Gestión de la capacidad tecnológica

ISO/IEC 27001:2022 ANEXO A.1.	ISO/IEC 27001:2013 ANEXO A.	DESCRIPCIÓN ANEXO A.1.
A 8.6. Gestión de capacidad	A 12.1.3. Gestión de capacidad	El uso de los recursos se debe monitorear y ajustar en función de las necesidades de capacidades actuales y previstas.
A 8.7. Protección contra malware	A 12.2.1. Controles contra códigos maliciosos	La protección contra el malware se debe implementar y respaldar mediante la conciencia adecuada del usuario.

2.4.3.1. Capacidades de recursos tecnológicos

El Ministerio garantiza la disponibilidad de los recursos tecnológicos institucionales, para el efecto la Oficina de Sistemas de Información:
• Monitorea las capacidades de los servicios tecnológicos, servidores de aplicación y bases de datos, canales de internet, almacenamientos, y el mantenimiento preventivo y correctivo de componentes tecnológicos y de usuario, plataformas de aíres acondicionados, planta eléctrica, entre otros.
• Identifica las necesidades a nivel tecnológico, con el fin de evitar potenciales indisponibilidades de los servicios de tecnológicos y de aplicación y sitios web, para mantener la continuidad ante los cambios en la infraestructura tecnológica.

2.4.3.2. Protección contra códigos maliciosos

El Ministerio implementa los controles informáticos y de ciberseguridad para prevenir la materialización de riesgos de seguridad digital, como resultado de eventos o incidentes que puedan generarse como resultado de la navegación en internet, recepción de correos electrónico

o instalación de software con vulnerabilidades técnicas, para el efecto cuenta en servidores, computadores y portátiles institucionales tienen instalado y actualizado el software de antivirus con actualización en línea, y monitoreo de la plataforma tecnológica y servicios tecnológicos.

2.4.4. Gestión de Vulnerabilidades y Remediaciones

ISO/IEC 27001:2022 ANEXO A.1.	ISO/IEC 27001:2013 ANEXO A.	DESCRIPCIÓN ANEXO A.1.
A 8.8. Gestión de Vulnerabilidades Técnicas	A 12.6.1. Gestión de las vulnerabilidades técnicas A 18.2.3. Revisión del cumplimiento técnico	Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a dichas vulnerabilidades y se deben adoptar las medidas apropiadas.

2.4.4.1. Evaluación de vulnerabilidades técnicas

La Oficina de Sistemas de Información coordina y monitorea la ejecución de las pruebas periódicas de vulnerabilidad técnica, de intrusión y en fuentes abiertas de los servicios de aplicación y sitios web, infraestructura tecnológica (On Premise y Nube) y usuarios fínales.

La Oficina de Sistemas de Información coordina la implementación de las acciones de remediación acorde con las capacidades tecnológicas y recursos disponibles, acorde con el alcance de implementación en el entorno de infraestructura tecnológica, monitoreo a plataforma tecnológica, o del ciclo de desarrollo de software.

2.4.4.2. Evaluación de vulnerabilidades técnicas

La Oficina de Sistemas de Información coordina y monitorea la ejecución de las pruebas periódicas de vulnerabilidad técnica, de intrusión y en fuentes abiertas de los servicios de aplicación y sitios web, infraestructura tecnológica (On Premise y Nube) y usuarios fínales.

2.4.4.3. Evaluación de sistemas, aplicaciones y sitios web

La Oficina de Sistemas de Información coordina la evaluación de vulnerabilidades y la implementación de las oportunidades de mejora del componente o servicio tecnológico, o el ajuste o corrección de acorde con el alcance del detalle de la vulnerabilidad para los nuevos desarrollos o ajustes a funcionalidades de aplicaciones y sitios web, y de hardening para servidores, servicios y componentes tecnológicos a nivel informático, de políticas de aseguramiento o ampliación de capacidades tecnológicas.

2.4.5. Configuración de servicios tecnológicos

ISO/IEC 27001:2022 ANEXO A.1.	ISO/IEC 27001:2013 ANEXO A.	DESCRIPCIÓN ANEXO A.1.
A 8.9. Gestión de la configuración	NUEVO	Las configuraciones, incluidas las configuraciones de seguridad de hardware, software, servicios y redes se deben establecer, documentar, implementar, monitorear y revisar.
A 8.10. Eliminación de información	NUEVO	La información almacenada en los sistemas de información, dispositivos o cualquier otro medio de almacenamiento se debe eliminar cuando ya no sea necesario.
A 8.11. Enmascaramiento de datos	NUEVO	El enmascaramiento de datos se debe utilizar de acuerdo con la política específica del tema de la organización sobre el control de acceso y otras políticas relacionadas con tema específicos, y los requisitos comerciales, teniendo en cuenta la legislación aplicable.
A 8.12. Prevención de fuga de datos	NUEVO	Las medidas de prevención de fugas de datos se deben implementar a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.
A 8.13. Copia de seguridad de la información	A 12.3.1 . Respaldo de la información	Las copias de seguridad de la información, el software y los sistemas se deben mantener y probar periódicamente de conformidad con la política específica sobre copias de seguridad sobre temas específicos.
A 8.14. Redundancia de las instalaciones de procesamiento de información	A 17.2.1. Disponibilidad de instalaciones de procesamiento de información	Las instalaciones de procesamiento de la información se deben implantar con redundancia suficiente para cumplir los requisitos de disponibilidad.
A 8.15. Registro - Inicio sesión	A 12.4.1. Registro de eventos A 12.4.2. Protección de la información de registro A 12.4.3. Registros del administrador y del operador	Los registros que guardan actividades, excepciones, fallas y otros eventos pertinentes se deben producir, almacenar, proteger y analizar.
A 8.16. Actividades de seguimiento	NUEVO	Se deben monitorear el comportamiento anómalo de las redes, los sistemas y las aplicaciones y se deben adoptar las medidas adecuadas para evaluar posibles incidentes de seguridad de la información.

ISO/IEC 27001:2022 ANEXO A.1.	ISO/IEC 27001:2013 ANEXO A.	DESCRIPCIÓN ANEXO A.1.
A 8.17. Sincronización de reloj	A 12.4.4. Sincronización de reloj	Los relojes de los sistemas de procesamiento de información utilizados por la organización se deben sincronizar con las fuentes de tiempo aprobadas.
A 8.18. Uso de Programas de Utilidad Privilegiados	A 9.4.4. Uso de programas utilitarios privilegiados	El uso de programas de utilidad que puedan ser capaces de anular los controles del sistema y de la aplicación debe restringirse y controlarse estrictamente.
A 8.19. Instalación de Software en Sistemas Operacionales	A 12.5.1. Instalación de software en sistemas operativos A 12.6.2. Restricciones sobre la instalación de software	Se deben implementar procedimientos y medidas para gestionar de forma segura la instalación de programas informáticos en los sistemas operativos.
A 8.20. Seguridad en Redes	A 13.1.1 Controles de redes	Las redes y los dispositivos de red deben estar asegurados, gestionados y controlados para proteger la información de los sistemas y las aplicaciones.
A 8.21. Seguridad de los servicios de red	A 13.1.2. Seguridad de los servicios de red	Se deben identificar, implementar y monitorear los mecanismos de seguridad, los niveles de servicios y los requisitos de servicio de los servicios de red.
A 8.22. Segregación de Redes	A 13.1.3. Separación en las redes	Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en las redes de la organización.
A 8.23. Filtrado web	NUEVO	El acceso a sitios web externos se deben gestionar para reducir la exposición a contenido malicioso.

La Oficina de Sistemas de Información es el área autorizada para:

- Adecuar la red y la infraestructura tecnológica del Ministerio, y administrar infraestructura On Premise y Nube.
- Implementar servicios y componentes tecnológicos y de seguridad digital.
- Instalar y desinstalar software operativo, de programación, utilitarios, aplicaciones y servicios web, software de usuario final, antivirus y antimalware, entre otros acorde con los requerimientos de la gestión tecnológica y de usuario final.
- Administrar las capacidades de los servicios de almacenamiento de información institucional.
- Realizar copias de seguridad de bases de datos y aplicaciones, y de servicios de las plataformas corporativas institucionales.
- Gestionar el acceso y autenticación usuarios en la red de datos y servicios tecnológicos de la entidad, aplicaciones y sitios web institucionales.
- Sincronizar el reloj de los dispositivos de red, servidores y equipos de usuarios final del Ministerio.
- Monitorear la navegación desde y hacia internet de aplicaciones y servicios web, de usuarios institucionales, la conexión remota, correo electrónico y la exposición de información institucional en fuentes abiertas; capacidades de servidores y disponibilidad de los servicios de aplicación y sitios web institucionales, entre otros.

2.4.6. Criptografía

ISO/IEC 27001:2022 ANEXO A.1.	ISO/IEC 27001:2013 ANEXO A.	DESCRIPCIÓN ANEXO A.1.
A 8.24. Uso de criptografía	A 10.1.1. Políticas sobre el uso de controles criptográficos A 10.1.2 . Gestión de llaves	Se deben definir e implementar normas para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas.

2.4.6.1. Política sobre el uso de controles criptográficos

En el Ministerio no se permite el uso de herramientas o mecanismos de encriptación o de firmas digitales diferentes a las definidas y autorizadas para los servicios de aplicación y sitios web administradas por la Oficina de Sistemas de Información.

2.4.6.2. Gestión de certificados de firma digital

El Ministerio dispone de la infraestructura tecnológica necesaria para soportar la operación de certificados de firma digital.

La Oficina de Sistemas de Información administra la plataforma para la gestión de firma digital para los aplicativos misionales que implementan dicha funcionalidad.

Los funcionarios y contratistas deben informar cualquier evento o incidente relacionado con el uso de la firma o certificado digital asignada al correo electrónico soportetecnico@mincit.gov.co.

2.4.6.3. Información encriptada

La Oficina de Sistemas de Información implementa los mecanismos y servicios tecnológicos requeridos para la transferencia o transmisión de información segura por medios electrónicos y de la información que se requiera en medios de almacenamiento removibles acorde con los requerimientos de transferencia a terceros y de transporte requeridos por el Grupo de Gestión Documental en coordinación del Grupo Administrativa.

2.4.7. Ambientes de desarrollo, pruebas y operación

ISO/IEC 27001:2022 ANEXO A.1.	ISO/IEC 27001:2013 ANEXO A.	DESCRIPCIÓN ANEXO A.1.
A 8.25. Ciclo de vida de desarrollo seguro	A 14.2.1. Política de desarrollo seguro	Se deben establecer e implementar normas para el desarrollo seguro de software y sistemas.
A 8.26. Requisitos de seguridad de la aplicación	A 14.1.2. Procedimientos de control de cambios en sistemas A 14.1.3. Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Los requisitos de seguridad de la información se deben identificar, especificar y aprobar al desarrollo o adquirir aplicaciones.
A 8.27. Arquitectura del sistema seguro y principios de ingeniería	A 14.2.5. Principios de construcción de los sistemas seguros	Los principios para la ingeniería de sistemas seguros se deben establecer, documentar, mantener e implementar a cualquier actividad de desarrollo de sistemas de información.
A 8.28. Codificación segura	NUEVO	Los principios de codificación segura se deben implementar al desarrollo de programas informáticos.
A 8.29. Pruebas de seguridad en desarrollo y aceptación	A 14.2.8. Pruebas de seguridad de sistemas A 14.2.9. Prueba de aceptación de sistemas	Los procesos de ensayo de seguridad se deben definir e implementar en el ciclo de vida del desarrollo.
A 8.30. Desarrollo subcontratado	A 14.2.7. Desarrollo contratado externamente	La organización debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas subcontratados.
A 8.31. Separación de los entornos de desarrollo, prueba y producción	A 12.1.4. Separación de los ambientes de desarrollo, pruebas y operación A 14.2.6. Ambiente de desarrollo seguro	Los entornos de desarrollo, ensayo y producción deben estar separados y protegidos.
A 8.32. Gestión del cambio	A 12.1.2. Gestión de cambios A 14.2.2. Procedimientos de control de cambios en sistemas A 14.2.3. Revisión técnica de las aplicaciones después de cambios en la plataforma de operación A 14.2.4. Restricciones en los cambios a los paquetes de software	Los cambios en las instalaciones de procesamiento y sistemas de información deben estar sujetos a procedimientos de gestión de cambios.

ISO/IEC 27001:2022 ANEXO A.1.	ISO/IEC 27001:2013 ANEXO A.	DESCRIPCIÓN ANEXO A.1.
A 8.33. Información de las pruebas	A 14.3.1 Protección de datos de prueba	La información de las pruebas se debe seleccionar, proteger y gestionar adecuadamente.
A 8.34. Protección de los sistemas de información durante las pruebas de auditoría	A 12.7.1. Controles de auditorías de sistemas de información	Las pruebas de auditoría y otras actividades de aseguramiento que impliquen la evaluación de los sistemas operativos se deben planificar y acordar conjuntamente entre el probador y la dirección adecuada.
A 8.32. Gestión del cambio	A 12.1.2. Gestión de cambios A 14.2.2. Procedimientos de control de cambios en sistemas A 14.2.3. Revisión técnica de las aplicaciones después de cambios en la plataforma de operación A 14.2.4. Restricciones en los cambios a los paquetes de software	Los cambios en las instalaciones de procesamiento y sistemas de información deben estar sujetos a procedimientos de gestión de cambios.
A 8.33. Información de las pruebas	A 14.3.1. Protección de datos de prueba	La información de las pruebas se debe seleccionar, proteger y gestionar adecuadamente.
A 8.34. Protección de los sistemas de información durante las pruebas de auditoría	A 12.7.1. Controles de auditorías de sistemas de información	Las pruebas de auditoría y otras actividades de aseguramiento que impliquen la evaluación de los sistemas operativos se deben planificar y acordar conjuntamente entre el probador y la dirección adecuada.

2.4.7.1. Entornos, Ambientes, capacidades y recursos

El Ministerio en su infraestructura tecnológica implementa de manera planificada las capacidades tecnológicas asociada para cada entorno de operación (On Premise y Nube) y ambientes de desarrollo, pruebas y producción. La Oficina de Sistemas de Información planifica y coordina la disponibilidad de capacidades y recursos requeridos para el desarrollo de aplicaciones y sitios web en todo el ciclo de vida tanto para desarrollos In House como para desarrollos con proveedores, y de seguridad informática. Para la implementación de los servicios de aplicación y sitios web se dispone con los ambientes de desarrollo, pruebas y producción, se configuran con los recursos requeridos para el acceso a recursos de procesamiento, instalación de software operativo y de desarrollo, bases de datos, y demás requeridos para el funcionamiento del servicio de aplicación y sitios web, ejecución del proceso de copias de seguridad o backup de servidores, monitoreo de la infraestructura y servicios en producción.

2.4.7.2. Aseguramiento de desarrollos de aplicación y sitios web

La Oficina de Sistemas de Información coordina con los desarrolladores In House y Proveedores de desarrollo la evaluación técnica de los servicios de aplicación y sitios web para asegurar el software ante defectos en la programación que afecten la integridad de los datos y su almacenamiento, uso de componentes vulnerables, debilidades de configuración en los servicios para el acceso y autenticación, entre otros; y la implementación de las remediaciones y pruebas finales para su puesta en producción. Una vez en producción las aplicaciones y sitios web deben incorporarse en la plataforma de seguridad digital para su monitoreo permanente y revisión de alertas de capacidades de los recursos tecnológicos asociados como parte de la gestión de vulnerabilidades.

2.4.7.3. Servicios en entorno nube

La Oficina de Sistemas de Información acorde con las necesidades institucionales gestiona la adquisición de las soluciones en nube requeridas para la gestión de la información institucional. Al igual que los servicios tecnológicos, aplicaciones y sitios web alojados en la infraestructura institucional, aplica los controles para asegurar en la adquisición el aseguramiento de la información institucional en entornos nube diferentes a los institucionales, que cubra entre otros aspectos, licenciamiento del software o servicio, bases de datos y copias de seguridad de la información, procesos de restauración de datos, gestión de cambios en los servicios y monitorea la ejecución de las pruebas periódicas de vulnerabilidad técnica.

2.4.7.4. Gestión de cambios de tecnologías de la información

La Oficina de Sistemas de Información coordina los cambios en la infraestructura tecnológica institucional relacionados con la incorporación de nuevos componentes tecnológicos y/o implementación de nuevos servicios tecnológicos o ajustes funcionales de aplicaciones o sitios web, actualización tecnológica de servicios y plataformas corporativas, incluye los requerimientos de capacidades tecnológicas necesarias, accesos de proveedores, copias de respaldo, y monitoreo de los servicios tecnológicos, y condiciones mínimas para garantizar la no la afectación de la operación de los procesos y servicios críticos, y mantener la disponibilidad, integridad o confidencialidad de la información.

2.4.7.5. Logs y registros de eventos en el entorno tecnológico

Todos los servicios tecnológicos, plataformas, aplicaciones y sitios web se encuentran incorporados en los equipos de seguridad digital para el monitoreo de los recursos tecnológicos asociados, navegación y tráfico, análisis de eventos y alertas generados como parte de su funcionamiento. La Oficina de Sistemas de Información permanentemente realiza el análisis de estos logs para verificar los controles informáticos implementados, revisar mejoras del control informático, mejoras de los servicios tecnológicos y de las aplicaciones y sitios web para determinar el alcance de las remediaciones y procesos de adecuación y actualización tecnológica, para asegurar la disponibilidad, integridad y confidencialidad de la información institucional.

2.5 HISTORIAL DE CAMBIOS

<table>
<tr><th>FECHA</th><th>VERSIÓN</th><th>DESCRIPCIÓN DEL CAMBIO</th></tr>
<tr><td>12/06/2026</td><td>0</td><td>Primera versión del documento para el nuevo Mapa de procesos.
Código anterior: GTI-DE-002.V02.

Para efectos de trazabilidad y soporte de la migración al nuevo aplicativo de administración de la documentación del Modelo Institucional de Operación (MIO), los siguientes fueron los responsables de la revisión y aprobación del documento migrado:

<table>
<tr><td>REVISÓ</td><td>APROBÓ</td></tr>
<tr><td>MARIA DEL ROSARIO CHACÓN

Cargo: Profesional especializado OSI</td><td>IVÓN CAROLINA RODRIGUEZ

Cargo: Jefe OSI</td></tr>
</table>
Desde la OAPS se asegura que el contenido corresponde a la última versión vigente en ISOlución al momento de la migración a MIOsoft.</td></tr>
</table>

FLUJO DE APROBACIÓN

ELABORÓ		APOYO OAPS		REVISÓ		APROBÓ	
Nombre:		Nombre:	Jefferson López	Nombre:		Nombre:	
Cargo:		Cargo:	Profesional Especializado	Cargo:		Cargo:	