TABLA DE CONTENIDO

LISTA DE VERSIONES

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
0	20/05/2016	Se elimina el documento de DI-GSI-001 Manual Políticas de Seguridad de la Información y se crea el documento DI-OPL-004 Políticas Específicas de Seguridad de la Información.
1	29/11/2017	1. Se actualiza el nombre de "POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN" por 2. "POLÍTICAS 3. ESPECÍFICAS DE SEGURIDAD Y 4. PRIVACIDAD DE LA INFORMACIÓN" Se elimina los capítulos 1 Objetivos y 2 Alcance. Se ajustan las definiciones de acuerdo con el contexto del documento. Se ajusta la estructura del documento de acuerdo con los lineamientos establecidos en DI-OPL-003 POLÍTICAS GENERALES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. 5. Se crea un objetivo por cada política.

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
		6. Se asigna un responsable por política. 7. Se estructuran las políticas relacionándolas con los controles del Anexo A de la NTC-ISO-27001:2013
2	31/12/2018	1. Actualización Logos Ministerio 2. Actualización de campos de etiquetado de información
3	6/08/2021	1. Cambio de Logo. 2. Se agrega capitulo Introducción 3. Se agrega capitulo Objetivos 4. Se ajusta objetivo General 5. Se defienden objetivos específicos 6. Se agrega capitulo Alcance 7. Se agrega capitulo Referencias legales y normativas. 8. Se agrega capitulo Gestiones SGSI 9. Se agrega capítulo 8 Vigencia 10. Se actualiza capitulo Definiciones 11. Se agrega capítulo de premisa de seguridad de la información 12. Numeración de políticas específicas por dominio. 13. Se realiza inclusión de controles sobre la relación con los proveedores.

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
		14. Aplicaciones de los criterios de creación de documentación accesibles

0 INTRODUCCIÓN

El presente documento se considera como una extensión de la POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, en la cual se plasman los compromisos de la alta dirección con el Subsistema de Gestión de Seguridad de la Información – SGSI en el Ministerio de las Culturas, las Artes y los Saberes (en adelante el "Ministerio" o la "Entidad"),

A continuación, se presentan las políticas específicas de seguridad y privacidad de la información, las cuales guiaran a los procesos y colaboradores en la implementación, cumplimiento y seguimiento de estas.

1 OBJETIVO GENERAL

Apoyar la implementación de los lineamientos establecidos en la Política General de Seguridad y Privacidad de la Información con el fin de proteger la información del acceso, uso y divulgación no autorizada, a través de la gestión que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Subsistema de Gestión de Seguridad de la información - SGSI del Ministerio.

1.1 OBJETIVOS ESPECÍFICOS

1.1.1 Definir lineamientos

Definir los lineamientos, documentos, procesos y roles necesarios para la protección de la información.

1.1.2 Cumplimiento legal y normativo

Cumplir con las disipaciones legales y normatividad vigente referentes a la seguridad de la información y el tratamiento de los datos personales.

2 ALCANCE

Esta política aplica a todos los colaboradores del Ministerio. De acuerdo con esto, es responsabilidad de los mismos cumplir todos los lineamientos establecidos en el Subsistema de Gestión de Seguridad de la Información - SGSI.

Por lo anterior es de obligatorio cumplimiento para todos los colaboradores del Ministerio y los terceros que interactúen con este.

3 DEFINICIONES

Amenaza: Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a colaboradores, procesos o entidades no autorizadas.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por un colaborador, proceso o entidad autorizada.

Dispositivo Móvil: Para efectos de este documento se hace referencia a computadores portátiles y tabletas personales o de propiedad del Ministerio.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información, inesperados o no deseados, que tiene probabilidad significativa de comprometer las operaciones del negocio y de amenazar la seguridad de la información.

Integridad: Propiedad de exactitud y completitud.

Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones.

Malware: Abreviatura de *malicious software*, este término engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento de este.

No repudio: Capacidad para corroborar que es cierta la reivindicación de que ocurrió un evento o una acción y las entidades que lo originaron.

Parte interesada: Persona u organización que puede afectar, estar afectada, o percibir que está afectada por una decisión o actividad.

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Sistema de información: Aplicaciones, servicios, activos de tecnologías de la información y otros componentes para manejar información.

Tercero: Persona natural o Jurídica delegada por el contratista o funcionario para cumplir labores o servicios contratados, que requiere acceder a los sistemas de información o servicios tecnológicos para desarrollar un proyecto, programa o actividad relacionada con la gestión del Ministerio.

Vulnerabilidad: Debilidad de un activo o de un control que puede ser explotad por una o más amenazas.

4 GESTIONES SGSI

4.1 GESTIÓN DE ACTIVOS

Orientar a los colaboradores del Ministerio en el levantamiento, clasificación y manejo de los activos de información que producen, almacenan, recolectan o custodian atendiendo las disposiciones normativas vigentes.

4.2 GESTIÓN DE RIESGOS

Definir una metodología para gestionar los riesgos de seguridad de la información y riesgos digitales en el Ministerio, con el fin de asegurar que el Subsistema de Gestión de Seguridad de la Información – SGSI logre los resultados previstos, se prevengan o reduzcan efectos indeseados y se consideren oportunidades que permitan el mejoramiento continuo.

4.3 GESTIÓN DE INCIDENTES

El objetivo de este procedimiento es propender porque los eventos, incidentes de seguridad de la información y debilidades de seguridad de la información sean detectados, analizados, mitigados y tratados eficiente y eficazmente.

4.4 GESTIÓN DE CONTINUIDAD DE LA OPERACIÓN

Definir las actividades que garanticen de manera eficiente la continuidad de la prestación de servicios, la operación de los sistemas de

información y los procesos, frente a un incidente que afecte el desarrollo cotidiano de la entidad en sus diferentes sedes.

4.5 PROTECCIÓN DE DATOS PERSONALES

Asegurar el adecuado tratamiento de los datos personales que se recolectan, almacenan, usan, circulan y suprimen en el ejercicio de las funciones propias del Ministerio, dando así cumplimiento de lo dispuesto en la Ley 1581 de 2012 y las demás normas concordantes.

4.6 GESTIÓN DE CULTURA Y APROPIACIÓN

Fomentar una Cultura de Seguridad de la información en los colaboradores del Ministerio que permita generar conciencia de sus deberes y responsabilidades frente a los activos de información y el Subsistema de gestión de seguridad de la información SGSI.

5 PREMISAS DE SEGURIDAD DE LA INFORMACIÓN

5.1 CONFIDENCIALIDAD

La información es conocida únicamente por las personas, usuarios o entidades autorizadas

CLASIFICACIÓN	DESCRIPCIÓN
INFORMACIÓN RESERVADA	Información disponible sólo para un proceso del Ministerio y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica. O si la información contiene datos personales sensibles o privados, por ejemplo: • Origen racial o étnico • Orientación política • Convicciones religiosas o filosóficas • Pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político • Datos relativos a la salud • Vida sexual • Datos biométricos. (huella dactilar, iris, etc.)
INFORMACIÓN CLASIFICADA	Información disponible para todos los procesos del Ministerio y que en caso de ser conocida por terceros

CLASIFICACIÓN	DESCRIPCIÓN
	sin autorización puede conllevar un impacto negativo para los procesos de esta. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario. O si la información contiene datos personales semiprivados: Cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas, financiero y crediticio de actividad comercial.
INFORMACIÓN PÚBLICA	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera del Ministerio, sin que esto implique daños a terceros ni a las actividades y procesos. O si la información contiene datos personales públicos, por ejemplo: • Nombres y apellidos. • Número de cédula. • Correo electrónico institucional.

CLASIFICACIÓN	DESCRIPCIÓN
	• Número telefónico institucional.

5.2 DISPONIBILIDAD

La información este accesible cuando se requiera y para los usuarios autorizados.

TIEMPO	DESCRIPCIÓN	CRITERIO	DETALLE
5 x 8	El activo de información debe estar disponible en horario laboral de lunes a viernes	BAJA	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.
6 x 10	El activo de información debe estar disponible en horario laboral de lunes a sábado	MEDIA	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
7 x 24	El activo de información debe estar disponible	ALTA	La no disponibilidad de la información puede conllevar un impacto negativo de

TIEMPO	DESCRIPCIÓN	CRITERIO	DETALLE
	los 7 días las 24 horas del día		índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.

5.3 INTEGRIDAD

La información este completa y sea exacta en todo momento; no se modifique sin autorización.

La integridad se refiere a la exactitud y completitud de la información (ISO 27000) esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción.

DESCRIPCIÓN	EXPLICACIÓN
ALTA	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
MEDIA	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.
BAJA	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.gg

6 POLÍTICAS ESPECIFICAS DE SEGURIDAD DE LA INFORMACIÓN

6.1 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

6.1.1 Organización Interna

Objetivo(s):	Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad y privacidad de la información dentro del Ministerio
Responsable(s):	• Oficina Asesora de Planeación
NTC-ISO-27001:2013 Anexo A	A.6.1.1 Roles y responsabilidades para la seguridad de la información. A.6.1.2 Separación de deberes. A.6.1.3 Contacto con las autoridades. A.6.1.4 Contacto con grupos de interés especial. A.6.1.5 Seguridad de la información en la gestión de proyectos.
Mediante la Resolución 4101 de 29 noviembre de 2018, se conforman y asignan funciones al comité Institucional de gestión y desempeño del Ministerio, el cual debe definir y asignar todas las responsabilidades de la seguridad de la información, teniendo en cuenta la segregación de funciones y separando las que se encuentren en conflicto. A. El Ministerio, a través de los diferentes procesos debe mantener o establecer el contacto con las autoridades pertinentes. • Documentar el procedimiento que especifique cuando y a través de que autoridades se debe contactar la entidad y como se	

deben reportar de manera oportuna los incidentes de seguridad de la información identificados.

B. La Oficina Asesora de Planeación y el Grupo de Gestión de Sistemas e Informática, deben mantener contacto apropiado con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad de la información, que permita, entre otros:

- Mejorar el conocimiento acerca de las buenas prácticas y permanecer al día con la información de seguridad pertinente.
- Asegurar que la comprensión del entorno de la seguridad de la información sea actual y esté completa.
- Recibir advertencias tempranas de alertas, avisos y parches acerca de ataques y vulnerabilidades.
- Obtener acceso a asesoría especializada en seguridad de la información.
- Compartir e intercambiar información acerca de nuevas tecnologías, productos, amenazas o vulnerabilidades.
- Brindar puntos de enlace adecuados cuando se trata con incidentes de seguridad de la información.

C. Todos los procesos del Ministerio deben incluir en la gestión de sus proyectos la seguridad de la información, independientemente del tipo de proyecto, para que se tenga en cuenta al menos lo siguiente:

- Los objetivos de la seguridad y privacidad de la información se incluyan en los objetivos del proyecto.

• La valoración de los riesgos de seguridad y privacidad de la información se lleva a cabo en una etapa temprana del proyecto, para identificar los controles necesarios. • La seguridad de la información sea parte de todas las fases de la metodología del proyecto aplicada.

6.1.2 Dispositivos móviles

Objetivo(s):	Adoptar una política y medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
Responsable(s):	• Grupo de Gestión Administrativa y de Servicios. • Grupo de Gestión de Sistemas e Informática.
NTC-ISO-27001:2013 Anexo A	A.6.2.1 Política para dispositivos móviles
A. Todo dispositivo móvil (computador portátil y tableta) que ingrese o se retire de las sedes del Ministerio deberá ser registrado por el personal encargado de la seguridad física en una base de datos en la que se pueda identificar como mínimo: • Fecha y hora de ingreso y salida. • Identificación de la persona que lo ingresa o retira. • Nombre(s) y Apellido(s) de la persona que lo ingresa o retira. • Dependencia a la que pertenece o se dirige. • Serial del dispositivo. • Marca del dispositivo.	

- Firma de la persona que lo ingresa o retira. Aplica para las minutas o formatos físicos.

B. Los dispositivos móviles propiedad del Ministerio, deben tener las restricciones respectivas para la instalación de software, protección contra códigos maliciosos, las actualizaciones del sistema operativo y de los programas instalados, así como un mecanismo que impida el robo o pérdida dentro de las instalaciones del Ministerio.

C. Los colaboradores responsables por los dispositivos móviles deberán comprometerse a protegerlos contra robo, pérdida o acceso no autorizado y de la información contenida en los mismos, especialmente cuando se dejan en automóviles y otras formas de transporte, habitaciones de hotel, centros de conferencias, lugares de reuniones, entre otros.

D. El uso de la red para conexión a internet de los dispositivos móviles propiedad de los colaboradores, deberá estar segmentada para proveer el servicio únicamente de internet, restringiendo el acceso a la red interna.

E. El uso de los dispositivos móviles debe ser con propósitos laborales.

F. La pérdida o robo de dispositivos móviles propiedad de la Entidad debe ser reportada:

- Grupo de Gestión Administrativa y de Servicios.
- Autoridades pertinentes

6.1.3 Teletrabajo

Objetivo(s):	Implementar una política y medidas de seguridad, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares donde se realiza teletrabajo.
Responsable(s):	• Grupo de Gestión Humana. • Grupo de Gestión de Sistemas e Informática.
NTC-ISO-27001:2013 Anexo A	A.6.2.2 Teletrabajo

A. Se debe documentar, implementar y garantizar mecanismos para la protección de la información a la que se tiene acceso y que sea procesada o almacenada en los lugares donde se realiza teletrabajo.
B. Se deben identificar y gestionar los riesgos de seguridad de la información concernientes al teletrabajo.
C. El colaborador en teletrabajo debe gestionar y procesar la información únicamente en los directorios y repositorios asignados para cada proceso.
D. Se debe verificar por lo menos los siguientes aspectos, antes, durante y posterior al teletrabajo:
   - Entorno físico de teletrabajo propuesto.
   - Los requisitos de seguridad de las comunicaciones, teniendo en cuenta la clasificación de la información y de los sistemas a los que se tendrá acceso.

- Certificar que el computador cumpla con las condiciones mínimas en cuanto a software y hardware, lo que incluye licencias, antivirus, actualizaciones, entre otras.
- Definir el trabajo permitido, horarios, clasificación de la información que se puede mantener, los sistemas y servicios internos a los que estén autorizados para acceder.
- La reglamentación y orientación sobre el acceso de la familia y los visitantes a los equipos y a la información.
- Posibilidad de monitorear y auditar las acciones realizadas en el teletrabajo.
- Revocación de los derechos de acceso y devolución de los equipos suministrados cuando finalice el periodo de teletrabajo.
- Uso adecuado del hardware y software entregado.

6.2 SEGURIDAD DEL RECURSO HUMANO

6.2.1 Antes de asumir el empleo

Objetivo(s):	Asegurarse que los colaboradores del Ministerio tomen conciencia de sus responsabilidades de seguridad y privacidad de la información, sean idóneos para los roles que se les considere.
Responsable(s):	• Grupo de Gestión Humana. • Grupo de Contratos y Convenios.
NTC-ISO-27001:2013 Anexo A	A.7.1.1 Selección A.7.1.2 Términos y condiciones del empleo

A. Se debe asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se les considera. B. Se debe llevar a cabo una verificación de los antecedentes de todos los candidatos a un empleo de acuerdo con las leyes, reglamentaciones y ética pertinentes. C. Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información. D. Se debe asegurar que todos los colaboradores y terceros a los que se brinde información confidencial deben firmar un acuerdo de confidencialidad y no divulgación antes de tener accesos a esta. E. Sede debe establecer las responsabilidades y derechos legales de los colaboradores con relación a leyes sobre derechos de autor o legislación sobre protección de datos.

6.2.2 Durante la ejecución del empleo

Objetivo(s):	Asegurarse que los colaboradores del Ministerio tomen conciencia de sus responsabilidades de seguridad y privacidad de la información y las cumplan.
Responsable(s):	• Grupo de Gestión Humana. • Grupo de Contratos y Convenios. • Grupo de Control Interno Disciplinario. • Oficina Asesora de Planeación.

	• Oficina de Control Interno.
NTC-ISO-27001:2013 Anexo A	A.7.2.1 Responsabilidades de la dirección A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información. A.7.2.3 Proceso disciplinario
A. Los colaboradores deben cumplir a cabalidad las políticas y procedimientos de seguridad y privacidad de la información establecidos por el Ministerio, entendiendo que cualquier violación puede acarrear procesos disciplinarios o sanciones de acuerdo con las formalidades establecidas institucionalmente. B. Todos los colaboradores del Ministerio deben recibir concientización y formación cuando sea pertinente en seguridad y privacidad de la información, así como la información de actualizaciones a las políticas y procedimientos de seguridad de la información relacionados con el desarrollo de su cargo u obligación. C. El Grupo de Control Interno Disciplinario debe contar con un proceso formal para emprender acciones contra empleados que hayan cometido una violación a la seguridad y privacidad e la información	

6.2.3 Terminación y cambio de empleo

Objetivo(s):	Proteger los intereses del Ministerio como parte del proceso de cambio o terminación de empleo o contrato.

Responsable(s):	• Grupo de Gestión Humana. • Grupo de Contratos y Convenios.
NTC-ISO-27001:2013 Anexo A	A.7.3.1 Terminación o cambio de responsabilidades de empleo.

A. Se debe comunicar y hacer cumplir al colaborador, las responsabilidades y deberes de seguridad y privacidad de la información que permanecen válidos después de la terminación o cambio de empleo o de contrato.
B. El Grupo de Gestión Humana y el Grupo de Contratos y Convenios a través de los supervisores de contratos, deben informar al Grupo de Gestión de Sistemas e Informática todas las novedades, desvinculaciones, terminaciones o cesiones de contrato, para retirar o modificar los privilegios de acceso físicos y lógicos.
C. Se debe documentar y comunicar las responsabilidades y deberes que son válidos después de la terminación o cambio de empleo.
D. Al finalizar su empleo, contrato o acuerdo, los colaboradores deben devolver todos los activos de información que se encuentren a su cargo y que fueron suministrados por el Ministerio para el cumplimiento de sus funciones u objeto del contrato.

6.3 GESTIÓN DE ACTIVOS

6.3.1 Responsabilidad por los activos

Objetivo(s):	Identificar los activos de información y definir las responsabilidades de protección apropiadas.

Responsable(s):	• Todas las dependencias procesos o sedes del Ministerio.
NTC-ISO-27001:2013 Anexo A	A.8.1.1 Inventario de activos. A.8.1.2 Propiedad de los activos. A.8.1.3 Uso aceptable de los activos. A.8.1.4 Devolución de activos.

A. Se deben identificar y mantener actualizados los activos de información por dependencia en el Ministerio, acorde con los procedimientos establecidos para ello.
B. Todos los activos de información deben tener un propietario asignado, así mismo, debe asegurarse que se encuentren protegidos contra amenazas.
C. Es responsabilidad de cada dependencia mantener actualizados los activos de información y de informar a la Oficina Asesora de Planeación y al Grupo de Gestión Documental cuando tengan cambios en su clasificación.
D. Es responsabilidad de cada dependencia informar cualquier novedad que pueda afectar la integridad, disponibilidad o confidencialidad de los activos de información.
E. Todos los colaboradores deben hacer buen uso de los activos de información a los cuales tienen acceso y que son propiedad del Ministerio, de igual forma, son responsables de cualquier uso que se les dé.
F. A continuación, se mencionan actos de mal uso, sin embargo, estos no se limitan a:

- Los recursos no podrán ser utilizados, para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, prácticas de juegos en línea, programas destructivos (virus), material político/religioso o cualquier otro uso que no esté vinculado con las labores institucionales.
- La navegación en Internet debe realizarse de forma razonable y con propósitos laborales. No se permite la navegación a sitios de alto riesgo, de contenido: pornográfico, terroristas, racistas, comunidades sociales, o cualquier contenido que represente riesgo para la red de la Entidad.
- No se permite él envió de correos desde el buzón institucional con contenido que atente contra la integridad humana de las personas o instituciones, como: pornográfico, terrorista, racista, o cualquier otro contenido que represente riesgo.
- Los correos electrónicos salientes de los buzones institucionales deben contar con la respectiva nota de confidencialidad y declinación de responsabilidades.
- No se permite la manipulación de las impresoras, ni la apertura de los computadores, cualquier reporte para solución de fallas debe ser reportado a la mesa de servicios.

G. Por motivos de seguridad, el Grupo de Sistemas e Informática se reserva el derecho de monitorear las cuentas de correo institucional y la navegación que presenten comportamiento sospechoso, lo anterior por posible causal que represente un incidente de seguridad.

6.3.2 Clasificación de la información

Objetivo(s):	Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para el Ministerio.
Responsable(s):	• Oficina Asesora de Planeación. • Grupo de Gestión Documental. • Grupo de Gestión de Sistemas e Informática.
NTC-ISO-27001:2013 Anexo A	A.8.2.1 Clasificación de la información. A.8.2.2 Etiquetado de la información. A.8.2.3 Manejo de activos.

A. Todos los activos de información se deben clasificar de acuerdo con los procedimientos o guías vigentes creados para tal fin, los responsables de realizar la clasificación, actualización y aprobación de los activos de información son todas las dependencias del Ministerio.
B. Se debe desarrollar e implementar procedimientos, mecanismos o herramientas para el etiquetado de la información acorde con los niveles de clasificación definidos y adoptados, dichas etiquetas permiten reconocer fácilmente la importancia del activo.
C. Para los sistemas de información que contienen información sensible o crítica se deben implementar mecanismos que indiquen la clasificación e identificación de la información.
D. La información que se intercambie con otras entidades debe incluir la clasificación correspondiente y se debe informar a su destinatario

la interpretación de la clasificación para que se asignen las protecciones necesarias.

6.3.3 Manejo de medios

Objetivo(s):	Evitar la divulgación, modificación, retiro o destrucción no autorizados de información almacenada en los medios.
Responsable(s):	• Todas las dependencias del Ministerio.
NTC-ISO-27001:2013 Anexo A	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. Cuando ya no se requiera la información contenida en un medio de almacenamiento reusable, de propiedad del Ministerio se debe borrar para que no sea recuperable.
B. Las unidades de almacenamiento suministradas por el Ministerio sólo deberán utilizarse para almacenar información relacionada con sus funciones u objeto del contrato, si estas salen del Ministerio deberán estar cifradas con el fin de evitar accesos no autorizados o divulgación de la información.
C. Los computadores de escritorio y equipos portátiles son de uso personal y exclusivo para el manejo de información del Ministerio, por tanto, no pueden ser prestados a personal ajeno al Ministerio, ni usados para almacenar o procesar información personal.

D. Si se almacena información clasificada con nivel alto en confidencialidad, disponibilidad o integridad en medios removibles se deben usar técnicas de cifrado para evitar accesos no autorizados o divulgación de la información en caso de pérdida, robo o extravío. E. Para los medios que contienen información confidencial, se deben almacenar y disponer de forma segura, mediante incineración, destrucción o proceso de borrado seguro, de acuerdo con las directrices del Grupo de Gestión Documental, Grupo de Gestión de Sistemas e Informática y de Gestión Ambiental del Ministerio. F. Los medios que contienen información (física o digital) se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte. G. Mitigar el riesgo de degradación de los medios, transfiriendo la información a medios diferentes antes de que se vuelva ilegible. H. Documentar el registro de los medios removibles para reducir la oportunidad de perdida de datos.

6.4 CONTROL DE ACCESO

6.4.1 Requisitos del negocio para control de acceso

Objetivo(s):	Limitar el acceso a información y a instalaciones de procesamiento de información.
Responsable(s):	• Grupo de Gestión de Sistemas e Informática.
NTC-ISO-27001:2013 Anexo A	A.9.1.1 Política de control de acceso. A.9.1.2 Acceso a redes y a servicios en red.

A. Se debe establecer mecanismos y herramientas para el control de acceso y creación de cuentas de todos los colaboradores nuevos.
B. Todos los accesos a la infraestructura física y lógica del Ministerio se deben realizar por herramientas autorizadas, no se permite el uso de software de acceso remoto no autorizado.
C. Todos los accesos a los sistemas de información, redes o servicios en red deben ser asignados acorde a los roles y responsabilidades de los colaboradores. Considerando el mínimo de privilegios necesarios para desempeñar sus funciones.
D. Los accesos a los sistemas de información y la red del Ministerio deben de estar debidamente autorizados y serán solicitados a través del aplicativo de mesa de ayuda únicamente por el Grupo de Gestión Humana, supervisores de los contratos o jefe inmediato según las obligaciones contractuales definidas y los procedimientos formalmente establecidos por el Grupo de Gestión de Sistemas e Informática.
E. Se debe documentar una política acerca del uso de las redes y de servicios de red, donde se indique los procedimientos de autorización, los controles establecidos, los medios usados para acceder (VPN, Wi-Fi), el monitoreo del uso, entre otros y en qué situaciones se pueden aplicar.
F. El acceso a los sistemas de información y dispositivos de red se debe realizar por usuarios administradores personalizados, se debe cambiar las credenciales de usuarios genéricos o por defecto.

G. Los accesos con privilegios especiales deben contar con la aprobación de la Coordinación del Grupo de Gestión de Sistemas e Informática y deben de estar debidamente justificados. H. Los responsables del manejo de usuarios privilegiados deben aceptar su responsabilidad frente al uso del usuario asignado. I. Los administradores funcionales de los sistemas de información deben realizar revisiones periódicas por lo menos una vez en el año de los usuarios activos en los diferentes sistemas de información, de dominio y de la red. J. Es responsabilidad de los jefes y coordinadores de cada dependencia, notificar a los administradores de los sistemas de información la desvinculación o retiro de un funcionario o contratista para que sean retirados los accesos de todos los sistemas incluidos los accesos físicos a las diferentes instalaciones del Ministerio. K. Se debe solicitar a los nuevos colaboradores el cambio inmediato de las credenciales entregadas al configurar el perfil. L. Todos los accesos físicos y lógicos serán inhabilitados el mismo día de terminación del contrato y deben ser configurados automáticamente desde la creación de las cuentas de usuario de los contratistas.

6.4.2 Gestión de acceso de usuarios

Objetivo(s):	Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.

Responsable(s):	• Grupo de Gestión de Sistemas e Informática.
NTC-ISO-27001:2013 Anexo A	A.9.2.1 Registro y cancelación del registro de usuarios A.9.2.2 Suministro de acceso de usuarios A.9.2.3 Gestión de derechos de acceso privilegiado A.9.2.4 Gestión de información de autenticación secreta de usuarios A.9.2.5 Revisión de los derechos de acceso de usuarios A.9.2.6 Retiro o ajuste de los derechos de acceso

A. Se debe documentar un proceso para la gestión de usuarios, dónde se detalle el uso de identificaciones únicas, así mismo, el uso de identificaciones compartidas o grupales por razones justificadas, establecer los tiempos de bloqueo o modificación de cuentas por inactividad, intentos fallidos, cambio de roles o empleo o retiro del Ministerio y realizar revisiones periódicas a los derechos de acceso a los sistemas de información o servicios, con el fin de mantener los privilegios y cuentas de usuario actualizadas.
B. Mantener un registro centralizado de los derechos de acceso suministrados para acceder a los sistemas de información y servicios a los colaboradores.
C. Los derechos de uso privilegiado sobre sistemas de información o servicios deben estar controlados y documentados mediante un proceso formal de autorización, asignando credenciales diferentes

para las actividades regulares, segmentados por cada sistema o proceso, donde se definan los requisitos para la expiración de estos, con especial atención a las cuentas configuradas para usuarios externos con propósitos específicos y por tiempo limitado.

D. Se deben implementar mecanismos para que los usuarios cambien su contraseña de acceso al usarla por primera vez en los sistemas de información o servicios a los que se les permita el acceso.
E. La información secreta para la autenticación temporal debe ser única para cada usuario y no debe ser fácil de adivinar, así mismo, solicitar un acuse de recibido de la misma.
F. Todas las credenciales por defecto del fabricante se deben cambiar después de la instalación de los sistemas de información, sistemas operativos, software o hardware que se use.
G. Los propietarios o custodios de los activos de información deben realizar revisiones periódicas a los derechos de acceso de los usuarios a intervalos regulares, así mismo, para las personas que los autoricen.
H. Para las cuentas privilegiadas se debe tener un registro de las modificaciones para la revisión periódica.

6.4.3 Responsabilidades de los usuarios

Objetivo(s):	Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.
Responsable(s):	• Todos los Colaboradores
NTC-ISO-27001:2013 Anexo A	A.9.3.1 Uso de información de autenticación secreta.

A. Todos los colaboradores deben cumplir con las políticas y lineamientos de seguridad de la información para el uso de información secreta para la autenticación (usuarios, contraseñas, token, tarjetas de proximidad, etc.), entre otras, las siguientes:

- Mantener la confidencialidad de la información para la autenticación, asegurándose que no sea divulgada o compartida con otros colaboradores o personal externo.
- Evitar escribir la información secreta (usuarios, contraseñas, etc.) en papeles o archivos electrónicos o almacenarla en los navegadores de internet.
- Ante cualquier sospecha de perdida de confidencialidad, se debe cambiar la contraseña.
- Evitar definir y usar contraseñas que sean fáciles de adivinar para otra persona, por ejemplo, nombres, números de teléfono, números de cedula, fechas de nacimiento, palabras relacionadas, entre otras.
- Evitar usar las mismas contraseñas para fines personales y laborales.
- La información confidencial del Ministerio, así como la información sensible de ciudadanos, no debe residir en servidores de internet, ni estar disponible para consulta en los sistemas públicos del Ministerio o que pueda ser accedida por medio de buscadores desde internet.

6.4.4 Control de acceso a sistemas y aplicaciones

Objetivo(s):	Evitar el acceso no autorizado a sistemas y aplicaciones.
Responsable(s):	• Grupo de Gestión de Sistemas e Informática.
NTC-ISO-27001:2013 Anexo A	A.9.4.1 Restricción de acceso a la información. A.9.4.2 Procedimiento de ingreso seguro. A.9.4.3 Sistema de gestión de contraseñas. A.9.4.4 Uso de programas utilitarios privilegiados. A.9.4.5 Control de acceso a códigos fuente de programas.

A. El acceso a la información y a las funcionalidades de las aplicaciones se debe restringir, de acuerdo, con los niveles de autorización para cada usuario o grupo de usuarios.
B. Cada aplicación o sistema de información debe considerar el suministro de menús para controlar el acceso a las funcionalidades de las aplicaciones, así como los derechos de los usuarios sobre las mismas (leer, escribir, borrar o ejecutar).
C. Controlar los accesos y usos desde otras aplicaciones y mantenerlos auditados y monitoreados.
D. En los procedimientos o interfaces de ingreso a las aplicaciones y sistemas de información:
   - Validar la información de ingreso solamente al completar todos los datos de entrada, en condiciones de error no se debe informar qué información es correcta o incorrecta.

- Se deben proteger contra intentos de ingreso mediante fuerza bruta.
- Almacenar un registro de los intentos éxitos y fallidos.
- Alertar cuando se detecten intentos potenciales o una violación exitosa de los controles de ingreso.
- No visualizar las contraseñas que se están ingresando.
- No transmitir contraseñas en texto claro en las redes o medios de comunicación.
- Finalizar las sesiones inactivas después de un periodo de inactividad de tiempo, con especial rigurosidad para lugares públicos, externos o dispositivos móviles.
- Bloquear los equipos de cómputo a los 3 minutos de inactividad

E. Las credenciales de los usuarios para acceder a los diferentes sistemas de información y la red del Ministerio son personales e intransferibles, estos no se deben compartir ni divulgar por ninguna razón.

F. Las credenciales de los colaboradores para acceder a los ambientes de pruebas y producción se deben diferenciar de forma que permitan identificar cada usuario para cada ambiente.

G. Las contraseñas de usuario para el acceso a la red y a todos los sistemas de información deben contar con los siguientes requisitos mínimos de seguridad:

- Alfanuméricas, mínimo un número, una letra en mayúscula y un carácter especial.
- Longitud mínima de ocho (8) caracteres.

- Cambio de contraseña cada sesenta (60) días.
- No puede contener el nombre de usuario, ni las palabras, ministerio, cultura o el año actual.
- No pueden tener caracteres consecutivos (ABCD, 12345)
- No se pueden usar las diez (10) últimas contraseñas.
- Al tercer (3°) intento de contraseña fallida, se debe bloquear el usuario.
- Se deben almacenar y transmitir de forma protegida.

H. Se debe restringir y controlar el uso de programar utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones, siguiendo las siguientes directrices mínimas:

- Usar procedimientos documentados de identificación, autenticación y autorización de los programas utilitarios.
- Limitar el uso de programas utilitarios al número mínimo de usuarios confiables y autorizados, teniendo en cuenta el tiempo de uso previsto.
- Retirar o inhabilitar todos los programas innecesarios.

I. Se debe controlar el acceso a códigos fuente de programas y elementos asociados (diseños, especificaciones, planes de prueba, resultados), para evitar la introducción de funcionalidades no autorizadas o cambios involuntarios, así mismo, para mantener la confidencialidad de la propiedad intelectual.

- Las librerías de programas fuente, no deberían estar contenidas en los ambientes de producción.

• Se debe documentar y hacer cumplir los procedimientos establecidos para la gestión de códigos fuente y las librerías de los programas. • Mantener un registro de auditoría de todos los accesos a la librería de fuentes de programas. • Se debe llevar un control de cambios adecuado para el mantenimiento y copia de las librerías de fuentes de programas. • El acceso a internet debe ser solicitado acorde a los procedimientos de gestión de accesos establecidos. • Los funcionarios y contratistas no deben ingresar a páginas de internet que contengan contenidos sexuales, racistas, o cualquier otro tipo de contenido ofensivo que vaya en contra de la ética, las leyes gubernamentales o la normatividad vigente.

6.5 CRIPTOGRAFÍA

6.5.1 Controles criptográficos

Objetivo(s):	Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad e integridad de la información.
Responsable(s):	• Grupo de Gestión de Sistemas e Informática.
NTC-ISO-27001:2013 Anexo A	A.10.1.1 Política sobre el uso de controles criptográficos. A.10.1.2 Gestión de llaves.

A. Se debe documentar, implementar y hacer cumplir el uso de controles criptográficos para la protección de la información. B. Validar que las llaves solo puedan ser usadas para una sola función y nunca reusadas, manteniendo así la integridad y no repudio. C. Documentar el clico de vida de las llaves criptográficas, desde su generación hasta el retiro y destrucción de estas.

6.6 SEGURIDAD FÍSICA Y DEL ENTORNO

6.6.1 Áreas seguras

Objetivo(s):	Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.
Responsable(s):	• Grupo de Gestión Administrativa y de Servicios. • Grupo de Gestión de Sistemas e Informática.
NTC-ISO-27001:2013 Anexo A	A.11.1.1 Perímetro de seguridad física. A.11.1.2 Controles de accesos físicos. A.11.1.3 Seguridad de oficinas, recintos e instalaciones. A.11.1.4 Protección contra amenazas externas y ambientales. A.11.1.5 Trabajo en áreas seguras.

	A.11.1.6 Áreas de despacho y carga.

A. Se deben definir y usar perímetros de seguridad y usarlos para proteger áreas que contengan información sensible o crítica e instalaciones de manejo de información, teniendo en cuenta lo siguiente:
   - En donde sea posible, el techo, las paredes y los pisos deber ser de construcción sólida.
   - Todas las puertas externas deberían tener mecanismos de control que eviten el acceso no autorizado.
   - Las puertas y ventanas se deben mantener cerradas con llave cuando no hay supervisión.
   - Para las ventanas se debe considerar protección contra acceso.
   - Se debe contar con un área de recepción con vigilancia para controlar el acceso físico a las instalaciones, restringiendo el acceso únicamente para el personal autorizado.
   - En donde sea necesario, se deben instalar sistemas para la detección de intrusos y ponerlas a prueba regularmente.

B. Se debe contar con un registro de acceso a las áreas seguras con:
   - Fecha y hora de entrada y salida
   - Nombre y firma de la persona autorizada

C. Todos los colaboradores deben estar plenamente identificados y se debe notificar al personal de seguridad si se encuentran visitantes no acompañados y sin identificación. D. No se debe permitir equipos fotográficos de video audio u otro equipo de grabación, tales como cámaras en dispositivos móviles.

6.6.2 Equipos

Objetivo(s):	Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.
Responsable(s):	• Grupo de gestión administrativa y de servicios. • Grupo de Gestión de Sistemas e Informática.
NTC-ISO-27001:2013 Anexo A	A.11.2.1 Ubicación y protección de los equipos. A.11.2.2 Servicios de suministro. A.11.2.3 Seguridad del cableado. A.11.2.4 Mantenimiento de equipos. A.11.2.5 Retiro de activos. A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones. A.11.2.7 Disposición segura o reutilización de equipos. A.11.2.8 Equipos de usuario desatendido.

	A.11.2.9 Política de escritorio limpio y pantalla limpia.

A. Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas, peligros del entorno y las posibilidades de acceso no autorizado, adoptando controles para minimizar el riesgo de amenazas físicas y ambientales como; robo, incendio, explosivos, humo, agua, polvo, vibración, interferencia en el suministro eléctrico o de comunicaciones, entre otros.
B. En los centros de cómputo o de cableado, se debe indicar la prohibición de acceso no autorizado, comer, consumir líquidos y fumar dentro o cerca de los mismos, además de contar con un sistema de registro de acceso por parte del personal autorizado.
C. Se debe hacer seguimiento a las condiciones ambientales como la temperatura y humedad, identificando oportunamente las condiciones que puedan afectar negativamente las instalaciones de los centros de cómputo o de cableado.
D. Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro (Electricidad, telecomunicaciones, ventilación, aire acondicionado,

etc.), cumpliendo con las especificaciones de los fabricantes de equipos y los requisitos para su adecuado funcionamiento.

E. Asegurar el funcionamiento apropiado de los equipos por medio de mantenimientos preventivos periódicos por parte de expertos técnicos, inspecciones o pruebas regulares, las cuales deben contar con un registro de cada uno de los eventos (Inspecciones, fallas reales, mantenimientos preventivos y correctivos).

F. El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información debe estar protegido durante todo su recorrido contra interceptación, interferencia o daño.

G. Se debe contar con sistemas de borrado seguro, cifrado de discos y un protocolo de destrucción de medios de almacenamiento de información sensible, software licenciado protegido por derechos de autor, instalados en equipos destinados para reutilización o equipos dañados.

H. Todos los colaboradores deben ser responsables de bloquear el escritorio en el momento de retirarse del puesto de trabajo y no dejar el equipo de cómputo desatendido, mediante el comando propio del sistema operativo o apagarlo.

I. Si el equipo va a permanecer inactivo por un periodo de tiempo superior a tres (4) horas deberá apagarse para evitar que sea usado por malware, así mismo, en cumplimiento de las recomendaciones del programa de ahorro y uso eficiente de la energía del Subsistema de Gestión Ambiental.

J. Se debe adoptar política de escritorio limpio para los documentos físicos, activos de información y pantalla limpia en los equipos de cómputo. K. Se debe cumplir por parte de los colaboradores del ministerio de la buena práctica de escritorio y pantalla limpios, reduciendo el riesgo de acceso no autorizado, pérdida y daño de la información durante y por fuera de las horas laborales normales. L. Se debe documentar la identidad del colaborador que recibe o entrega el equipo de cómputo a su cargo. M. Se debe registrar el retiro y devolución de los activos de información de las sedes del Ministerio.

6.7 SEGURIDAD DE LAS OPERACIONES

6.7.1 Procedimientos operacionales y responsabilidades

Objetivo(s):	Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.
Responsable(s):	• Grupo de Gestión de Sistemas e Informática.
NTC-ISO-27001:2013 Anexo A	A.12.1.1 Procedimientos de operación documentados. A.12.1.2 Gestión de cambios. A.12.1.3 Gestión de capacidad. A.12.1.4 Separación de los ambientes de desarrollo, pruebas, y operación.

A. Se deben documentar los procedimientos de las actividades operacionales especificando las instrucciones para:
   - Instalación y configuración de sistemas.
   - Copias de respaldo (Backup)
   - Requisitos de programación, incluidas las interdependencias con otros sistemas.
   - las instrucciones para manejo de errores u otras condiciones excepcionales.
   - contactos de apoyo y de una instancia superior (escalamiento), incluidos los contactos de soporte externo, en el caso de dificultades operacionales o técnicas inesperadas.
   - procedimientos de reinicio y recuperación del sistema para uso en el caso de falla del sistema.

B. Los cambios en la organización se deben controlar, en los procesos de negocio, instalaciones y en los sistemas de información que afectan la seguridad de la información, identificándolos, planificándolos, poniéndolos a prueba y aprobándolos formalmente, así como valorando los impactos potenciales e incluir procedimientos y responsabilidades para abortar cambios no exitosos, eventos no previstos y recuperarse de ellos.

C. Se debe hacer seguimiento al uso de recursos, hacer los ajustes y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema, considerando documentar planes de gestión de capacidad para los sistemas críticos de la misionalidad.

D. Se deben separar los ambientes de desarrollo, prueba y producción, bajo niveles, reglas y procedimientos documentados que disminuyan el riesgo de pérdida operativa y de información en los pasos de migración entre etapas.
E. Los Colaboradores no deben instalar ningún tipo de canales de transmisión, módems, ni cambiar la configuración de sus equipos sin la previa aprobación del Grupo de Gestión de Sistemas e Informática.
F. Los Colaboradores no deben instalar ningún tipo de canales de transmisión, módems, ni cambiar la configuración de sus equipos sin la previa aprobación del Grupo de Gestión de Sistemas e Informática.
G. Los usuarios deben asumir un comportamiento cuidadoso, ético, responsable y diligente en el uso de Internet. Está prohibido el acceso a sitios que no tengan relación con la actividad que se desarrolla para el Ministerio, en especial el acceso a material inapropiado como páginas pornográficas, páginas ofensivas, chats y foros no autorizados por el Ministerio.

6.7.2 Protección contra códigos maliciosos

Objetivo(s):	Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
Responsable(s):	• Grupo de Gestión de Sistemas e Informática
NTC-ISO-27001:2013 Anexo A	A.12.2.1 Controles contra códigos maliciosos.

A. Todos los equipos utilizados por los colaboradores que están conectados a la red del Ministerio ya sean de propiedad o no, deben estar actualizados con software antivirus y con las últimas actualizaciones de este, además de complementar con capacitación para la toma de conciencia de los usuarios y controles para evitar la instalación o detección de software no autorizado.
B. Debe implementar controles de detección, prevención y recuperación, para proteger al Ministerio contra ataques de códigos maliciosos.
C. Todo el software instalado en los computadores debe estar previamente autorizado creando listas blancas de aplicaciones, así mismo, se deben realizar revisiones periódicas para asegurar que se cumpla la política.
D. Los colaboradores tienen prohibido descargar, utilizar e instalar software externo en los recursos tecnológicos del Ministerio a menos que el software haya sido analizado en busca de código malicioso, aprobado e instalado por el Grupo de Gestión de Sistemas e Informática.
E. Se deben implementar controles que impidan la modificación de las configuraciones del equipo de cómputo o del software instalado con énfasis en el sistema operativo y antivirus.
    - Los usuarios deben asegurarse de que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio o instalación de código malicioso.

- El Grupo de Gestión de Sistemas e Informática se regirá por las siguientes directrices:
  - Contar con software de protección debidamente licenciado, activo y actualizado contra código malicioso en todos sus servidores, equipos de cómputo y los archivos intercambiados por correo electrónico tanto entrantes como salientes.
  - Establecer mecanismos para mantener actualizados todos los sistemas de procesamiento de información (parches de software y actualizaciones).
  - Impedir la instalación de códigos móviles tales como cookies, ActiveX, a menos que se encuentre dentro del listado de sitios web permitidos y/o aceptados.
  - Contar con análisis de páginas web para determinar el software malicioso.

6.7.3 Copias de respaldo

Objetivo(s):	Proteger contra la pérdida de datos.
Responsable(s):	• Grupo de Gestión de Sistemas e Informática
NTC-ISO-27001:2013 Anexo A	A.12.3.1 Respaldo de la información
A. Se debe contar con una política de respaldo para todos los sistemas de información y repositorios de información institucional; Plenamente documentadas, definidas y publicadas en el sistema de calidad que se adapten a las necesidades de las diferentes áreas del Ministerio.	

B. Se debe contar con una metodología de pruebas y una adecuada infraestructura para la creación de copias de respaldo, con protocolos de restauración periódica y una adecuada área remota de almacenamiento, así como sistemas de cifrado para información de alta confidencialidad y su respectivo periodo de retención. C. Es responsabilidad de los colaboradores realizar copias de respaldo de la información contenida en sus computadores o en los dispositivos de almacenamiento a su cargo.

6.7.4 Registro y seguimiento

Objetivo(s):	Registrar eventos y generar evidencia.
Responsable(s):	• Grupo de Gestión de Sistemas e Informática
NTC-ISO-27001:2013 Anexo A	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. A.12.4.4 Sincronización de relojes.
A. Se debe identificar los sistemas críticos del Ministerio y llevar una metodología de revisión y custodia de eventos (Event Logs), que permita, identificar las actividades por usuario, excepciones, fallas y eventos de seguridad que no den espacio a la alteración, uso no autorizado o repudio, en caso de presentarse materialización del riesgo y ser utilizados como medio probatorio. B. Se debe mantener los relojes de todos los equipos y dispositivos, sincronizados con una única fuente de referencia (http://horalegal.inm.gov.co/), de acuerdo con un proceso	

documentado con los requisitos internos y externos que mantengan la exactitud del tiempo y permitan la correlación de eventos y logs.

C. Se debe restringir a los colaboradores la administración de fecha y hora de los sistemas de información, aplicaciones o equipos de cómputo a su cargo.

6.7.5 Control de software operacional

Objetivo(s):	Asegurarse de la integridad de los sistemas operativos.
Responsable(s):	• Grupo de Gestión de Sistemas e Informática
NTC-ISO-27001:2013 Anexo A	A.12.5.1 Instalación de software en sistemas operativos.

A. Se debe mantener un procedimiento de control de instalación y cambios de los sistemas operativos del Ministerio administrado por expertos técnicos; para mantener operativas las aplicaciones basadas en estos y que permitan procedimientos de retroceso (RollBack) exitosos.

B. Es responsabilidad de los expertos técnicos, mantener custodiadas copias idénticas de sistemas operativos que respondan a eventos de contingencia y disminuyan el impacto en caso de falla irreversible.

C. Las aplicaciones y software del sistema operativo solo se debe implementar o actualizar, después de realizar pruebas exitosas.

D. Se debe realizar pruebas periódicas de las copias de los sistemas operativos con el fin de validar su disponibilidad e integridad

E. No está permitida la descarga de software, archivos de audio, medios audiovisuales que atenten contra los derechos de autor, la infraestructura tecnológica y la seguridad de la información del Ministerio.

6.7.6 Gestión de vulnerabilidad técnica

Objetivo(s):	Prevenir el aprovechamiento de las vulnerabilidades técnicas.
Responsable(s):	• Grupo de Gestión de Sistemas e Informática
NTC-ISO-27001:2013 Anexo A	A.12.6.1 Gestión de las vulnerabilidades técnicas. A.12.6.2 Restricciones sobre la instalación de software.
A. Se debe contar con una metodología de identificación de vulnerabilidades técnicas alineada con la gestión de incidentes, para exponer la situación de riesgo frente a ellas y permitirle a los responsables aplicar los controles de mitigación que correspondan, previa evaluación en un ambiente de pruebas (implementación de parches, cambios de librerías y todo cambio de tipo técnico que de espacio a la incertidumbre en el resultado esperado), además, de	

evaluar el riesgo de implementación frente al riesgo que acarrea la vulnerabilidad, priorizando los sistemas que se encuentren en alto riesgo. B. Se debe mantener, evaluar y mejorar las reglas y privilegios para la instalación de software en los equipos de los colaboradores del Ministerio, todo lo anterior dentro del marco de la mayor restricción posible. C. Si está disponible una actualización de firmware o actualización de sistemas operativos o de información, se deberá validar los riesgos del despliegue, se deberá probar y evaluar antes de su instalación. D. Se debe identificar los riesgos asociados, las acciones a tomar y definir una línea de tiempo para reaccionar a las notificaciones de vulnerabilidades técnicas. E. Se debe establecer e implantar reglas para la instalación de software por parte de los colaboradores.

6.7.7 Consideraciones sobre auditorías de sistemas de información

Objetivo(s):	Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.
Responsable(s):	• Grupo de Gestión de Sistemas e Informática
NTC-ISO-27001:2013 Anexo A	A.12.7.1 Controles de auditorías de sistemas de información.
A. Se debe evaluar el impacto sobre los servidores que requieren la ejecución de sistemas de auditoría para priorizar rendimiento de los sistemas críticos sobre la seguridad de la información que	

gestionan, evitando así interrupciones en los procesos de la Entidad.

6.8 SEGURIDAD DE LAS COMUNICACIONES

6.8.1 Gestión de la seguridad de las redes

Objetivo(s):	Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.
Responsable(s):	• Grupo de Gestión de Sistemas e Informática
NTC-ISO-27001:2013 Anexo A	A.13.1.1 Controles de redes. A.13.1.2 Seguridad de los servicios de red. A.13.1.3 Separación en las redes.

A. Las redes de datos y comunicaciones del Ministerio deben estar gestionadas y controladas para protección de la información y sus aplicaciones, gestión de red y configuración de redes virtuales o creación de subredes que permitan separar los servicios de información, usuarios y sistemas.
B. El Ministerio excluye cualquier tipo de responsabilidad por la información que pueda ser vista y descargada desde internet, solo es permitido el uso de internet para fines propios de la actividad que el usuario realiza para el Ministerio y no para fines personales.
C. Por seguridad y para propósitos de mantenimiento, se podrá monitorear en cualquier momento el tráfico de la red. Esta labor será realizada solo por personal autorizado, garantizando a los

usuarios que no existirá revisión interna de archivos o documentos de carácter personal sin la autorización previa y expresa del usuario.

D. Se debe disponer de una zona desmilitarizada o DMZ, entre la red interna y la red externa (internet) con el objetivo limitar conexiones desde la red interna hacia Internet y conexiones desde internet hacia la red interna del Ministerio.

E. Se deben establecer controles especiales para salvaguardar la confidencialidad e integridad de los datos que pasan sobre las redes.

F. Se debe identificar los mecanismos de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de red.

G. Se debe separar en las redes los grupos de servicios de información usuarios y sistemas de información.

6.8.2 Transferencia de información

Objetivo(s):	Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.
Responsable(s):	• Grupo de Gestión de Sistemas e Informática • Grupo de Gestión de Contratos y Convenios • Grupo de Gestión Administrativa y de Servicios

NTC-ISO-27001:2013 Anexo A	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. A.13.2.4 Acuerdos de confidencialidad o de no divulgación.

A. El Ministerio a través de sus responsables, debe mantener , revisar y documentar regularmente las políticas y procedimientos formales de transferencia de información, entre la organización y las partes externas que utilizan la infraestructura de telecomunicaciones (correo electrónico empresarial y privado, telefonía IP y telefonía celular) para minimizar el riesgo de pérdida de información y credibilidad, además se debe reforzar periódicamente en los funcionarios los beneficios del buen uso y protección de la información.
B. Los canales de red utilizados para la transferencia de información deberán contar con un mecanismo que no permita la fuga o interceptación de información, en su defecto la información que viaja por estos deberá estar cifrada.
C. Generar acuerdos para tratar la transferencia segura de información entre la entidad y las partes externas.
D. El Ministerio a través de los procesos responsables de la contratación y adquisición de servicios, debe velar por la gestión de los acuerdos de confidencialidad y no divulgación de la información.

6.9 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

6.9.1 Requisitos de seguridad de los sistemas de información

Objetivo(s):	Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.
Responsable(s):	• Grupo de Gestión de Sistemas e Informática
NTC-ISO-27001:2013 Anexo A	A.14.1.1 Análisis y especificación de requisitos de seguridad de la información. A.14.1.2 Seguridad de servicios de las aplicaciones en redes públicas. A.14.1.3 Protección de transacciones de los servicios de las aplicaciones.

A. El Grupo de Gestión de Sistemas e Informática con el apoyo de Subsistema de gestión de la seguridad de la información debe:

- Definir, documentar y hacer cumplir los requisitos de seguridad para los nuevos sistemas y las mejoras de los existentes, incluyendo las configuraciones de red para proteger la información que se administra en las bases de datos y que son transmitidas por los medios físicos, los cuales a su vez deben estar controlados frente a la posibilidad de ser intervenidas, para disminuir el riesgo de fraude, no repudio, modificaciones y divulgación no

autorizadas, transmisión incompleta, enrutamiento errado o alterado, duplicación o reproducción de mensajes no autorizada. • Ejecutar revisiones periódicas al licenciamiento de software y eliminar o desinstalar de los equipos de cómputo, el software que no se encuentre licenciado por el Ministerio. • Autorizar el uso de software libre previo estudio de seguridad de la información. • Definir y establecer los estándares y procedimientos para el desarrollo, mantenimiento y adquisición de portales web y sistemas de información, incluyendo la custodia del código fuente, ambientes de prueba, control de cambios y toda la infraestructura tecnológica relacionada, de conformidad con las mejoras prácticas del mercado y reglas internacionales de seguridad informática. • Recomendar, asesorar y avalar lo relativo a la adquisición y distribución de licencias de software, equipos de seguridad, comunicaciones y otros dispositivos que compongan la plataforma tecnológica. • Realizar la supervisión técnica de los contratos de desarrollo de software del Ministerio.

6.9.2 Seguridad en los procesos de desarrollo y soporte

Objetivo(s):	Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.
Responsable(s):	• Grupo de Gestión de Sistemas e Informática

NTC-ISO-27001:2013 Anexo A	A.14.2.1 Política de desarrollo seguro. 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. A.14.2.5 Principios de construcción de los sistemas seguros. A.14.2.6 Ambiente de desarrollo seguro. A.14.2.7 Desarrollo contratado externamente. A.14.2.8 Pruebas de seguridad de sistemas. A.14.2.9 Prueba de aceptación de sistemas.
A. El Ministerio debe definir, documentar, mantener y hacer cumplir estrictas reglas para el desarrollo de los sistemas de información propios (incluyendo la infraestructura) o de terceros (Paquetes de Software), para controlar los cambios dentro del ciclo de desarrollo, con especial énfasis en las aplicaciones críticas, las cuales deben ser sometidas a pruebas de aseguramiento para minimizar el impacto en las operaciones que se soportan sobre estos desarrollos y asegurando la información que se maneja en ellos. B. Las actividades de instalación de software y actualización de los archivos de configuración del sistema solo pueden ser realizadas por personal del Grupo de Gestión de Sistemas e Informática, por tanto,	

está prohibido modificar, alterar o programar cualquier tipo de configuración.

C. El Grupo de Gestión de Sistemas e Informática debe definir, documentar y revisar los requisitos mínimos de seguridad requeridos para el acceso a la red de los equipos externos o dispositivos móviles propios y de terceros.

D. Se debe establecer, documentar y mantener principios para la construcción de sistemas seguros, los cuales debe ser aplicados cualquier implementación de sistemas de información.

E. El Ministerio debe establecer los acuerdos de licenciamiento, propiedad de los códigos y derechos de propiedad intelectual, relacionados con el contenido contratado.

F. El Ministerio debe solicitar y verificar el suministro de evidencias de los umbrales de seguridad para establecer los niveles mínimos aceptables y las pruebas de protección contra vulnerabilidades conocidas.

G. El grupo de gestión de sistemas e informática debe realizar las pruebas de aceptación del desarrollo de acuerdo con los criterios establecidos.

6.9.3 Datos de prueba

Objetivo(s):	Asegurar la protección de los datos usados para pruebas.
Responsable(s):	• Grupo de Gestión de Sistemas e Informática
NTC-ISO-27001:2013	A.14.3.1 Protección de datos de prueba.

Anexo A	
A. El Ministerio debe asegurar que las bases de datos utilizadas en ambientes de prueba no realicen ninguna operación directa sobre la base de datos de producción. B. Los datos de prueba no deben contener información sensible, de ser necesario este contenido se deben utilizar mecanismos de enmascaramiento o sustitución de datos.	

6.10 RELACIONES CON LOS PROVEEDORES

6.10.1 Seguridad de la información en las relaciones con los proveedores

Objetivo(s):	Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.
Responsable(s):	• Todas las dependencias del Ministerio.
NTC-ISO-27001:2013 Anexo A	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. A.15.1.3 Cadena de suministro de tecnología de información y comunicación.
A. Todo proveedor debe cumplir con los lineamientos establecidos en la contratación pública y los procedimientos del Ministerio.	

B. Los accesos a las instalaciones o sistemas de información únicamente serán entregados si son requeridos para el cumplimiento de sus obligaciones contractuales siguiendo los procedimientos establecidos para tal fin.
C. Los proveedores deben cumplir las políticas de seguridad de la información y están obligados a reportar fallas o incidentes que se presenten o evidencien en la ejecución de sus actividades en el Ministerio.
D. El Grupo de Contratos y Convenios deberá establecer los lineamientos para el cumplimiento de la política de seguridad y privacidad de la información, requisitos legales y regulatorios en todos los contratos con proveedores o terceros.
E. El Grupo de Contratos y Convenios deberá establecer los lineamientos para el cumplimiento de los requisitos legales y regulatorios relacionados con la protección de datos personales, información, derechos de autor y propiedad intelectual.
F. El desarrollo de aplicativos o sistemas de información diseñado por terceros debe estar bajo estándares de desarrollo del Grupo de Gestión de Sistemas e Informática y alineado a las políticas de seguridad y privacidad de la información.
G. El Grupo de Contratos y Convenios deberá establecer acuerdos de confidencialidad con proveedores y terceros en los contratos que se ejecuten.

6.10.2 Gestión de la prestación de servicios de proveedores

Objetivo(s):	Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.
Responsable(s):	• Todas las dependencias del Ministerio.
NTC-ISO-27001:2013 Anexo A	A.15.2.1 Seguimiento y revisión de los servicios de los proveedores. A.15.2.2 Gestión de cambios en los servicios de los proveedores.

A. El Ministerio a través de los procesos debe realizar seguimiento, revisión y auditaría a la prestación de los servicios realizados por los terceros o proveedores.
B. El Grupo de Gestión de Sistemas e Informática deberá establecer y documentar controles para el acceso de los proveedores o terceros a la información o servicios tecnológicos del Ministerio.
C. Todas las dependencias del Ministerio solicitaran sensibilización periódica en los temas del SGSI a sus proveedores y terceros.
D. Todo proveedor o tercero debe estar informado de las políticas de seguridad y privacidad de la información y lineamientos del SGSI para cumplimiento de su contrato.

6.11 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

6.11.1 Gestión de incidentes y mejoras en la seguridad de la información

Objetivo(s):	Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.
Responsable(s):	• Oficina Asesora de Planeación • Grupo de Gestión de Sistemas e Informática • Grupo de Gestión Administrativa y de Servicios.
NTC-ISO-27001:2013 Anexo A	A.16.1.1 Responsabilidades y procedimientos. A.16.1.2 Reporte de eventos de seguridad de la información. A.16.1.3 Reporte de debilidades de seguridad de la información. A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos. A.16.1.5 Respuesta a incidentes de seguridad de la información. A.16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información. A.16.1.7 Recolección de evidencia.
A. Se deben establecer responsabilidades y procedimientos documentados para asegurar la respuesta rápida, eficaz y ordenada	

a los incidentes de seguridad de la información; teniendo en cuenta las siguientes etapas:

- Planificación y preparación.
- Seguimiento, detección, análisis y reporte de eventos e incidentes.
- Registro de actividades de gestión de incidentes.
- Manejo de evidencia forense.
- Valoración y toma de decisiones sobre eventos de seguridad de la información.
- Respuesta, escalamiento y recuperación controlada.
- Comunicación interna y externa.

B. Los colaboradores del Ministerio deben informar a través de los canales definidos todos los eventos de seguridad de la información que sean evidenciados.

C. Se debe definir tiempos de respuesta y atención a los eventos presentados, procedimientos de escalamiento y declaración de contingencia.

D. Se debe documentar y mantener actualizada una gestión de conocimiento alimentada por los incidentes o eventos presentados.

E. Se debe implementar un punto de contacto para la detección y reporte de incidentes de seguridad de la información.

F. Mantener documentado y disponible un contacto con autoridades, grupos de interés que manejen cuestiones relacionados con seguridad de la información e incidentes.

6.12 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO

6.12.1 Continuidad de seguridad de la información

Objetivo(s):	La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.
Responsable(s):	• Todas las dependencias del Ministerio.
NTC-ISO-27001:2013 Anexo A	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.

A. Se debe documentar y desarrollar los lineamientos y procedimientos necesarios para la eventual interrupción de servicios, planes de recuperación ante desastres que permitan retornar a la operación normal de los sistemas de información del Ministerio.
B. Los proveedores de servicios críticos deberán contar con planes de continuidad que permitan desarrollar pruebas periódicas de los mismos.
C. Se debe realizar un análisis de riesgos, identificar controles para los mismos, diseñar, documentar y realizar pruebas que permitan

minimizar los riesgos y continuar la prestación de servicios del Ministerio al momento de presentarse un evento.

D. Los planes de continuidad de negocio deben ser documentados, publicados y de acceso a todos los colaboradores del Ministerio.
E. Los planes de continuidad de negocio deben ser analizados, probados y actualizados de forma periódica o cuando ocurra un evento que afecte la prestación u operación de los servicios del Ministerio.
F. Se debe generar informes o reportes de las pruebas realizadas a los planes de continuidad que incluyan recomendaciones, lecciones aprendidas, acciones de mejora y esta información debe ser acceso a los colaboradores interesados o participantes de las pruebas.
G. Se debe definir un equipo para la planeación y ejecución de las pruebas de redundancia tecnológica u operativa del Ministerio.
H. Los participantes de las pruebas deberán recibir sensibilización en las políticas de seguridad, sus responsabilidades, procesos y roles al presentarse un evento que interrumpa la prestación de servicios del Ministerio.

6.12.2 Redundancias

Objetivo(s):	Asegurar la disponibilidad de instalaciones de procesamiento de información.
Responsable(s):	• Grupo de Gestión de Sistemas e Informática
NTC-ISO-27001:2013 Anexo A	A.17.2.1 Disponibilidad de instalaciones de procesamiento de información.

El Grupo de Gestión de Sistemas e Informática deberá Implementar la infraestructura necesaria para contar con redundancia en los sistemas de información o servicios críticos del Ministerio. A. Establecer y documentar un equipo y un programa de pruebas a las redundancias tecnológicas u operativas con las que cuenta el Ministerio. B. Probar periódicamente las arquitecturas o servicios redundantes asegurando su operación luego de presentarse un evento.

6.13 CUMPLIMIENTO

6.13.1 Cumplimiento de requisitos legales y contractuales

Objetivo(s):	Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.
Responsable(s):	• Todas las dependencias del Ministerio.
NTC-ISO-27001:2013 Anexo A	A.18.1.1 Identificación de la legislación aplicable y de los requisitos Contractuales. A.18.1.2 Derechos de propiedad intelectual. A.18.1.3 Protección de registros. A.18.1.4 Privacidad y protección de información de datos personales. A.18.1.5 Reglamentación de controles criptográficos.

A. Toda dependencia que por su naturaleza genere o manipule información impresa y física de los ciudadanos, funcionarios y contratistas catalogada como sensible de acuerdo con la Ley 1581 de 2012, debe abstenerse de reutilizar este papel como reciclable y a su vez debe garantizar la destrucción de estos documentos cuando ya no sean requeridos para ningún proceso y trámite en el Ministerio.
B. El SGSI deberá definir y documentar una política de protección de datos personales. Velar por su publicación y divulgación a todos los ciudadanos y colaboradores del Ministerio.
C. Todos los sistemas de información que capturen datos personales de ciudadanos deben cumplir con la política de tratamiento y el manual de tratamiento y protección de datos personales definida por el Ministerio.
D. El SGSI con el apoyo de la Oficina Asesora Jurídica debe documentar y actualizar la herramienta de verificación de requisitos legales, estatutarios y contractuales.
E. El SGSI debe generar conciencia en los colaboradores en temas de propiedad intelectual y derechos de autor.

6.13.2 Revisiones de seguridad de la información

Objetivo(s):	Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.

Responsable(s):	• Oficina Asesora de Planeación • Oficina de Control Interno • Grupo de Control Interno Disciplinario • Grupo de Gestión de Sistemas e Informática
NTC-ISO-27001:2013 Anexo A	A.18.2.1 Revisión independiente de la seguridad de la información. A.18.2.2 Cumplimiento con las políticas y normas de seguridad. A.18.2.3 Revisión del cumplimiento técnico.

A. La oficina de control interno deberá realizar de forma periódica auditorías internas verificando la correcta implementación del Subsistema de Gestión de Seguridad de la Información - SGSI, así como el cumplimiento de políticas y anexos generados.
B. El Grupo de Gestión de Sistemas e Informática deberá verificar periódicamente que los Sistemas de información y la Infraestructura tecnológica cumplen con los lineamientos de seguridad de la información.
C. El Subsistema de gestión de seguridad de la información deberá realizar inspecciones al cumplimiento de los lineamientos establecidos bajo su gestión.
D. El incumplimiento de las Políticas podrá dar lugar a un proceso disciplinario para los funcionarios y se podrá convertir en un incumplimiento del contrato respecto de los contratistas, que pueda dar lugar a la imposición de sanciones e incluso su terminación, sin perjuicio de la iniciación de otro tipo de acciones a las que haya lugar.

7 REFERENCIAS LEGALES Y NORMATIVAS

- Gobierno Digital
- MSPI Modelo de Seguridad y Privacidad de la Información
- MIPG Modelo Integrado de Planeación y Gestión
- ISO/IEC 27001:2013
- ISO/IEC 27002:2015
- Ley 1341 de 2009 Principios y conceptos de las TI
- Ley 1273 de 2009 Protección de la información y los datos (información como bien jurídico)
- Ley 1712 de 2014 Transparencia y acceso a la información
    - Decreto 103 de 2015 Reglamenta la ley 1712 de 2014
    - Resolución 3564 reglamenta los aspectos relacionados con la ley 1712
- Ley 1581 de 2012 Protección de datos personales
    - Decreto 1377 de 2013 Reglamenta parcialmente la ley 1581
- Decreto 1499 de 2017 Actualiza el Modelo Integrado de Planeación y Gestión – MIPG
- Decreto 1008 de 2018 Lineamientos generales de la política de gobierno digital
    - DUR 1078 de 2015 Decreta la estructura del sector de tecnologías de la información y las comunicaciones
- CONPES 3854 de 2017 Política nacional de seguridad digital
- CONPES 3701 de 2015 Lineamientos de políticas para ciberseguridad y ciberdefensa

8 VIGENCIA

Las políticas específicas de seguridad y privacidad de la Información, cuenta con la revisión y aprobación del Comité de Desarrollo Administrativo Institucional y se encuentra vigente a partir de su publicación a través del aplicativo del Sistema Integrado de Gestión Institucional.

Será revisada a intervalos planificados, o cuando se produzcan cambios significativos en los procesos, infraestructura física o tecnológica o todo aspecto que afecte la misionalidad del Ministerio.