TABLA DE CONTENIDO

1. INTRODUCCIÓN 2
2. OBJETIVO 2
3. ALCANCE 2
4. DEFINICIONES 3
5. MARCO LEGAL Y NORMATIVO 7
6. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL 9
7. DESARROLLO 10
7.1. LINEAMIENTOS DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 10
7.2. LINEAMIENTOS DE SEGURIDAD DE LOS RECURSOS HUMANOS 11
7.3. LINEAMIENTOS DE SEGURIDAD PARA LA GESTIÓN DE ACTIVOS 14
7.4. LINEAMIENTOS DE SEGURIDAD PARA EL CONTROL DE ACCESO. 17
7.5. LINEAMIENTOS DE SEGURIDAD PARA EL USO DE RECURSOS CRIPTOGRÁFICOS. 21
7.6. LINEAMIENTOS DE SEGURIDAD FÍSICA Y DEL ENTORNO 21
7.7. LINEAMIENTOS DE SEGURIDAD DE LAS OPERACIONES 26
7.8. LINEAMIENTOS DE SEGURIDAD DE LAS COMUNICACIONES 31
7.9. LINEAMIENTOS DE SEGURIDAD PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS 34
7.10. LINEAMIENTOS DE SEGURIDAD PARA LA RELACIÓN CON LOS PROVEEDORES 38
7.11. LINEAMIENTOS PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 39
7.12. LINEAMIENTOS PARA DEFINIR LOS ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE LA OPERACIÓN 39
7.13. LINEAMIENTOS PARA EL CUMPLIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN 41

1. INTRODUCCIÓN

El Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, reconoce que la información que gestiona es uno de los activos más importantes para su funcionamiento y que ésta puede ser de naturaleza legal, estratégica, financiera, operativa y en algunos casos corresponder a datos personales de servidores públicos, contratistas y grupos de interés. Igualmente, es consciente de las amenazas que enfrenta dicho activo y de las consecuencias a las que se expone la Entidad cuando ésta no cuenta con las medidas de seguridad adecuadas.

En ese sentido, se hace necesario propender por la seguridad y privacidad de la información en el MinTIC, teniendo presente que la vulneración se encuentra en cualquier estado de su ciclo de vida (creación, procesamiento, almacenamiento, transmisión, utilización o destrucción), puede llegar a tener impactos a nivel legal, de imagen, operacional, en el cumplimiento de la misión y los objetivos estratégicos de la Entidad.

Teniendo en cuenta lo anterior, el presente Manual establece los principios orientadores de seguridad que buscan garantizar la disponibilidad, integridad, confidencialidad, privacidad, continuidad, autenticidad y no repudio de la información del Ministerio, así como dar lineamientos para la aplicación de mecanismos que eviten la vulneración de la seguridad y privacidad de la información, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información – SGSI.

2. OBJETIVO

Establecer los lineamientos para la adecuada gestión de la seguridad y privacidad de la información en el MinTIC, enmarcados en la implementación de un Sistema de Gestión de Seguridad de la Información, basado en la identificación y valoración de los riesgos asociados a ella, propendiendo por la protección de su confidencialidad, integridad, disponibilidad, privacidad, continuidad, autenticidad y no repudio y por el cumplimiento de la normatividad vigente aplicable|.

3. ALCANCE

Los lineamientos contenidos en el presente manual se aplican a la información circulante en el Mapa de Procesos, Tablas de Retención Documental – TRD, documentos de apoyo y demás información

que administre, proteja y preserve el Ministerio y cualquier entidad que ejerza en su nombre a través de la recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información, con personal interno o externo, en el desarrollo de la misión institucional y el cumplimiento de sus objetivos estratégicos.

4. DEFINICIONES

Con el objeto de precisar el alcance de los principales conceptos utilizados en este documento, se transcriben las definiciones *[ISO 27000:2013]*:

- **Activo**: Se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas) que tienen un valor para la entidad.
- **Activo crítico**: Instalaciones, sistemas y equipos los cuales, si son destruidos, o es degradado su funcionamiento o por cualquier otro motivo no se encuentran disponibles, afectaran el cumplimiento de los objetivos estratégicos del Ministerio.
- **Administración de Riesgos**: Se entiende por administración de riesgos, como el proceso de identificación, control, minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar la información o impactar de manera considerable la operación. Dicho proceso es cíclico y deberá llevarse a cabo en forma periódica.
- **Amenaza**: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la entidad.
- **Análisis de Impacto al Negocio**: Es una metodología que permite identificar los procesos críticos que apoyan los productos y servicios claves, las interdependencias entre procesos, los recursos requeridos para operar en un nivel mínimo aceptable y el efecto que una interrupción del negocio podría tener sobre ellos.
- **Autenticidad**: Busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- **Centro de cableado**: El centro de cableado es el lugar donde se ubican los recursos de comunicación de Tecnología de información, como (Switch, patch, panel, UPS, Router, Cableado de voz y de datos).
- **Ciberactivo crítico**: Ciberactivo que es crítico para la operación de un activo crítico.
- **Ciberactivo**: Se identifica como foco de la ciberseguridad los activos digitales como datos, dispositivos y sistemas que permiten a la organización cumplir con sus objetivos de negocio.
- **Ciberseguridad**: Es el proceso de proteger los activos de información por medio del tratamiento de las amenazas a la información que es procesada, almacenada y/o transportada a través de sistemas de información interconectados.
- **Comité de Seguridad de la Información**: El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas sustantivas del Ministerio, destinado a apoyar el cumplimiento de las normas, procesos y procedimientos de seguridad de la información.

- **Confiabilidad de la Información**: Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
- **Confidencialidad**: Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Datacenter**: Se denomina también Centro de Procesamiento de Datos (CPD) a aquella ubicación o espacio donde se concentran los recursos necesarios (TI) para el procesamiento de la información de una organización.
- **Disponibilidad**: Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.
- **Dispositivos móviles**: Equipo celular smartphone, equipos portátiles, tablets, o cualquiera cuyo concepto principal sea la movilidad, el cual permite almacenamiento limitado, acceso a internet y cuenta con capacidad de procesamiento.
- **DMZ**: Sigla en inglés de DeMilitarized Zone hace referencia a un segmento de la red que se ubica entre la red interna de una organización y la red externa o internet de VPN.
- **Equipos activos de red:** Son todos los dispositivos que hacen la distribución de las comunicaciones a través de la red de datos.
- **Evaluación de Riesgos**: Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operación de la entidad.
- **Incidente de Seguridad**: Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Información**: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
- **Integridad**: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **Legalidad**: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la entidad.
- **Medio removible**: Los dispositivos de almacenamiento removibles son dispositivos de almacenamiento independientes del computador y que pueden ser transportados libremente. Los dispositivos móviles más comunes son: Memorias USB, Discos duros extraíbles, DVD y CD.
- **Mesa de Servicios**: Constituye el único punto de contacto con los usuarios finales para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información. Es a través de la gestión proactiva de la Mesa de Servicios que la Oficina de Tecnologías de la Información recolecta las necesidades que tienen dependencias en cuanto a los recursos tecnológicos.
- **No repudio:** El emisor no puede negar que envió porque el destinatario tiene pruebas del envío. El receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor pueda negar tal envío.

- **Paneles de conexión (patch panel):** Elemento encargado para la organización de conexiones en la red.
- **Plan de Continuidad de Negocio**: Actividades documentadas que guían a la Entidad en la respuesta, recuperación, reanudación y restauración de las operaciones a los niveles pre-definidos después de un incidente que afecte la continuidad de las operaciones.
- **Plan de tratamiento de riesgos**: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
- **Propietario del riesgo**: Persona o proceso con responsabilidad y autoridad para gestionar un riesgo.
- **Protección a la duplicación**: Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- **Oficial de Seguridad de la información**: Es la persona que cumple la función de supervisar el cumplimiento de la Política, coordinar el Comité de Seguridad de la Información y de asesorar en la materia a los integrantes de la entidad que así lo requieran.
- **Riesgo**: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.
- **Sistema de Información**: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales. Conjunto de aplicaciones que interactúan entre sí para apoyar un área o proceso del Ministerio.
- **Tecnologías de la Información**: Las tecnologías de la información y las Comunicaciones - TIC, Nuevas Tecnologías de la Información y de la Comunicación - NTIC, agrupan los elementos y las técnicas utilizadas en el tratamiento y la transmisión de las informaciones, principalmente de informática, internet y telecomunicaciones.
- **Test de penetración**: Es un ataque dirigido y controlado hacia componentes de infraestructura tecnológica para revelar malas configuraciones y vulnerabilidades explotables.
- **VPN**: Red virtual privada por sus siglas en ingles Virtual Private Network.
- **Alta Dirección:** Persona o grupo de personas que dirigen y controlan al más alto nivel una entidad (Ministro, Viceministros, Secretaria General y Direcciones).
- **Autenticación:** Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.
- **Cifrado:** Método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.
- **Control:** Son todas aquellas políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

- **Control Correctivo:** Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.
- **Control Detectivo**: Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.
- **Control Disuasorio:** Control que reduce la posibilidad de materialización de una amenaza, por ejemplo, por medio de avisos disuasorios.
- **Control Preventivo:** Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.
- **Código malicioso:** Es un código informático que crea brechas de seguridad para dañar un sistema informático.
- **Dato Personal:** Cualquier información vinculada o que pueda asociarse a una o a varias personas naturales determinadas o determinables. Debe entonces entenderse el "dato personal" como una información relacionada con una persona natural (persona individualmente considerada).
- **Dato Personal Público:** Toda información personal que es de conocimiento libre y abierto para el público en general.
- **Dato Personal Privado:** Toda información personal que tiene un conocimiento restringido, y en principio privado para el público en general.
- **Dato Semiprivado:** Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su Titular sino a cierto sector o grupo de personas o a la sociedad en general.
- **Datos Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.
- **Evento:** Es el suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.
- **Evento de Seguridad de la Información:** Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o falla de salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

- **Fiabilidad**: Se define como la probabilidad de que un bien funcione adecuadamente durante un período determinado bajo condiciones operativas específicas (por ejemplo, condiciones de presión, temperatura o velocidad).
- **Impacto:** Resultado de un incidente de seguridad de la información.
- **Partes interesadas:** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- **Privacidad de la información:** El derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de Gobierno Digital la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
- **Terceros:** Personas naturales o jurídicas que tienen un contrato tercerizado y prestan un servicio a la entidad y hacen uso de la información y los medios tecnológicos dispuestos por la entidad.
- **Teletrabajo**: Es una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación – TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo.
- **Vulnerabilidad**: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

5. MARCO LEGAL Y NORMATIVO

El MinTIC referencia las siguientes normas y modelos para la gestión de la seguridad y privacidad de la información, en la Entidad:

- **Constitución Política de Colombia.** Artículo 15.
- **Ley 44 de 1993.** Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor).
- **Ley 527 de 1999.** Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- **Ley 594 de 2000.** Por medio de la cual se expide la Ley General de Archivos.
- **Ley 850 de 2003.** Por medio de la cual se reglamentan las veedurías ciudadanas
- **Ley 1266 de 2008.** Por la cual se dictan las disposiciones generales del Ha□beas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

- **Ley 1221 del 2008.** Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
- **Ley 1273 de 2009.** Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- **Ley 1341 de 2009.** Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones - TIC- Se crea la agencia Nacional de espectro y se dictan otras disposiciones.
- **Ley 1437 de 2011.** Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.
- **Ley 1474 de 2011.** Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- **Ley 1581 de 2012.** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Ley 1712 de 2014.** Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- **Ley 1915 de 2018.** Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- **Ley 1952 de 2019.** Por medio de la cual se expide el código general disciplinario
- **Decreto 2609 de 2012.** Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- **Decreto 0884 del 2012.** Por el cual se reglamenta parcialmente la Ley 1221 del 2008.
- **Decreto 1377 de 2013.** Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- **Decreto 886 de 2014.** Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- **Decreto 103 de 2015.** Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- **Decreto 1074 de 2015.** Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- **Decreto 1078 de 2015.** Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 1080 de 2015.** Por medio del cual se expide el Decreto Reglamentario del Sector Cultura.
- **Decreto 1081 de 2015.** Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
- **Decreto 728 de 2017.** Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo

de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico

- **Decreto 1499 de 2017.** Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- **Decreto 1008 del 2018.** Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- **Resolución 2999 del 2008.** Por el cual se adoptan las políticas de seguridad para el manejo de la información y se dictan otras normas para el uso y administración de los bienes y servicios informáticos del Ministerio TIC.
- **Resolución 2034 de 2016.** Por la cual se adoptó el Modelo de Responsabilidad Social Institucional en el Ministerio TIC.
- **Resolución 2007 de 2018.** Por la cual se actualiza la política de tratamiento de datos personales del Ministerio/Fondo TIC.
- **Resolución 911 de 2018.** Por la cual se actualiza el Modelo Integrado de Gestión del MinTIC.
- **Resolución 2133 de 2018.** Por la cual se establecen las condiciones especiales del Teletrabajo en el Ministerio de Tecnologías de la Información y las Comunicaciones, y se deroga las resoluciones No 3559 y 4950 de 2013, 2313 y 494 de 2014 y 2787 de 2016.
- **Resolución 512 de 2019.** Por la cual se adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se definen lineamientos frente al uso y manejo de la información.
- **CONPES 3701 de 2011.** Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- **CONPES 3854 de 2016.** Política Nacional de Seguridad digital.

6. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

El Ministerio de Tecnologías de la Información y las Comunicaciones, mediante la adopción e implementación del Modelo de Seguridad y Privacidad de la Información enmarcado en el Sistema de Gestión de Seguridad de la información, protege, preserva y administra la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información que circula en el mapa de procesos, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales previniendo así incidentes y dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información, propendiendo así al acceso, uso efectivo y apropiación masiva de las TIC, a través de políticas y programas, para mejorar la calidad de vida de cada colombiano y el incremento sostenible del desarrollo del país.

7. DESARROLLO

7.1. LINEAMIENTOS DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Código: SI-A.6.1. – Organización Interna.

Propósito: Establecer un marco de referencia de gestión y operación de seguridad y privacidad de la información en la Entidad.

Lineamientos:

a. Los activos de información deberán estar bajo la responsabilidad del Líder de Proceso para evitar conflicto y reducir oportunidades de modificación (intencional o no) no autorizada o mal uso de los activos de información del Ministerio.
b. El Oficial de Seguridad de la Información debe mantener y documentar los contactos con autoridades (Policía Nacional, INTERPOL, Bomberos, Defensa Civil, Grupos de atención de desastres, etc.) u otros especializados y asociaciones profesionales para que puedan ser contactados de manera oportuna en el caso de que se presente un incidente de seguridad de la información que requiera de asesoría externa, siempre que esta sea informada por el líder del proceso afectado.
c. El Ministerio a través del Oficial de Seguridad de la Información y demás personal que este determine debe mantener contacto con grupos de interés especializados en seguridad y privacidad de la información, con el fin de compartir e intercambiar conocimientos en pro a la mejora continua del Sistema de Gestión de Seguridad de la Información del Ministerio.
d. La Oficina Asesora de Planeación debe incluir en la metodología gestión de proyectos del Ministerio, los aspectos relacionados con la seguridad y Privacidad de la Información en todas las etapas del proyecto; además prever los planes necesarios para garantizar la continuidad de los servicios asociados al proyecto, una vez se encuentre en la etapa productiva.

Código: SI-A.6.2 – Dispositivos Móviles y Teletrabajo.

Propósito: Establecer un marco de referencia para la operación dispositivos móviles que gestionen información propia del Ministerio.

Lineamientos:

a. La Oficina de Tecnologías de la Información, debe establecer un procedimiento que brinde a las dependencias la orientación con respecto a la autorización, configuración y uso de los dispositivos móviles de propiedad servidores públicos, contratistas o terceros que requieran tener acceso a la información a través del portafolio de servicios tecnológicos del Ministerio.
b. La Oficina de Tecnologías de la Información, debe implementar las medidas necesarias de seguridad y privacidad, para propender por la protección de la información gestionada mediante aplicaciones y sistemas de información.

c. La Oficina de Tecnologías de la Información, debe mantener un inventario actualizado de los dispositivos móviles autorizados para acceder a la red corporativa, asociando el número de ticket de la mesa de servicios por el cual fue autorizada la solicitud.
d. La Oficina de Tecnologías de la Información, debe establecer un checklist dentro del procedimiento, con el fin de validar que los computadores portátiles personales cuenten con software licenciados y antivirus actualizado.
e. Los computadores portátiles de propiedad de los colaboradores no deberán estar incluidos en el dominio mintic.gov.co o cualquiera que funcione dentro del Ministerio, para conectarse a los servicios de la red de datos deberán realizar solicitud a la mesa de servicios y cumplir con los lineamientos referentes a seguridad de la información.
f. La Oficina de Tecnologías de la Información, debe proporcionar a los dispositivos móviles tipo portátil, las herramientas Ofimáticas, Antivirus y de almacenamiento en nube licenciadas por la Entidad.
g. Para la modalidad de Teletrabajo, la Oficina de Tecnologías de la Información debe definir y proveer las herramientas tecnológicas para teletrabajar, estableciendo las condiciones de seguridad y privacidad de la información, de acuerdo a la Resolución 2133 de 2018 y las enmarcadas en el Libro Blanco del Teletrabajo o cualquiera que la adicione, modifique o complemente.
h. El Grupo Interno de Trabajo de Gestión del Talento Humano, debe mantener actualizado el procedimiento de teletrabajo y en especial los aspectos relacionados con la seguridad y privacidad de la información.
i. El Grupo Interno de Trabajo de Gestión del Talento Humano, debe establecer los mecanismos necesarios para sensibilizar a los teletrabajadores y aspirantes a teletrabajo en temas de seguridad y privacidad de la información.
j. Para la modalidad de Teletrabajo, la Oficina de Tecnologías de la Información debe establecer mecanismos de monitoreo sobre las conexiones y los servicios tecnológicos a los que el teletrabajador tiene acceso.

7.2. LINEAMIENTOS DE SEGURIDAD DE LOS RECURSOS HUMANOS

Código: SI-A.7.1 – Antes de asumir el empleo
Propósito: Establecer lineamientos para asegurar que el personal a contratar cumpla con las políticas de seguridad y privacidad de la Información del Ministerio.
Lineamientos:

a. El Grupo Interno de Trabajo de Gestión del Talento Humano, debe definir formalmente un mecanismo de verificación del personal en el momento en que se postula al cargo. Dicho mecanismo deberá incluir los aspectos legales y procedimentales de vinculación del Ministerio y los que dicte la Función Pública.
b. El Grupo Interno de Trabajo de Contratación, debe definir una lista de verificación que contengan los aspectos necesarios para la revisión de los antecedentes del personal a

contratar por prestación de servicios de acuerdo a lo que dicta la Ley y la reglamentación vigente.

c. Los procesos de selección de personal de servidores públicos y contratistas de prestación de servicios deben contener la autorización para el tratamiento de los datos personales de acuerdo con la Política de tratamiento de datos personales del Ministerio y de acuerdo a lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios.
d. El Grupo Interno de Trabajo de Contratación y el Grupo Interno de Trabajo de Gestión del Talento Humano, deben establecer los mecanismos o controles necesarios para proteger la confidencialidad y reserva de la información contenida en las historias laborales y expedientes contractuales.
e. Todo servidor público o contratista debe firmar un documento de acuerdo de confidencialidad y no divulgación de la información con el Ministerio, dicho documento debe reposar en la historia laboral o expediente contractual según sea el caso.
f. El Grupo Interno de Trabajo de Gestión del Talento Humano, debe incluir dentro del manual de funciones las responsabilidades con respecto al cumplimiento de las políticas de seguridad y privacidad de la información, así como todos los lineamientos en el marco del Sistema de Gestión de Seguridad de la Información.
g. El Grupo Interno de Trabajo de Contratación, debe incluir en el pliego de condiciones y estudios previos para la contratación, las obligaciones referentes a las políticas, lineamientos y directrices en materia de seguridad de la información que dicte el Ministerio.
h. El Grupo Interno de Trabajo de Gestión del Talento Humano, y el Grupo Interno de Trabajo de Contratación deben dar a conocer durante la inducción las responsabilidades u obligaciones en materia de la seguridad de la información y aclarar que estas se extienden más allá de los límites del Ministerio y del horario normal de trabajo o de ejecución del objeto contractual.

Código: SI-A.7.2 – Durante la ejecución del empleo
Propósito: Establecer los lineamientos sobre las responsabilidades de los colaboradores del Ministerio con la seguridad de la información, de acuerdo con las políticas y procedimientos establecidos.
Lineamientos:

a. Una vez formalizado el proceso de vinculación, el jefe inmediato, supervisor o el delegado de la dependencia para tal fin, debe solicitar el paquete OTI, la apertura del inventario y demás servicios que requiera el colaborador para la ejecución de sus funciones u obligaciones contractuales.
b. El Oficial de Seguridad de la Información en conjunto con la Oficina Asesora de Prensa deben diseñar e implementar un Plan de cambio y cultura organizacional en apropiación del SGSI, el cual se debe ejecutar durante la vigencia al interior del Ministerio.

c. El Grupo Interno de Trabajo de Gestión del Talento Humano o el supervisor del contrato deben propender que los colaboradores del Ministerio y usuarios de terceras partes que desempeñen funciones en el mismo, reciban entrenamiento y actualización periódica en materia de Seguridad de la Información.
d. El Grupo Interno de Trabajo de Gestión del Talento Humano en conjunto con el Oficial de Seguridad de la Información, deben establecer un curso virtual en la Universidad Corporativa relacionado con seguridad y privacidad de la información.
e. En lo pertinente al incumplimiento y desacato de las políticas de la seguridad de la información, se aplicará lo establecido en los procedimientos destinados para tal fin, por los entes de control interno del Ministerio, enmarcados en Ley 1952 de 2019, sus decretos reglamentarios o cualquiera que la modifique, adicione, derogue o subrogue.

Código: SI-A.7.3 – Terminación y cambio de empleo
Propósito: Establecer los lineamientos sobre las responsabilidades de los colaboradores del Ministerio con la seguridad de la información que permanecen validos después de la terminación o cambio de empleo.
Lineamientos:

a. El jefe inmediato o a quien este delegue debe recoger y custodiar la información propia del Ministerio, que se encuentra en gestión del servidor público, cuando existe una novedad de retiro, investigación, inhabilidades, o cambio de funciones.
b. El supervisor del contrato o a quien este delegue deben recoger y custodiar la información del Ministerio bajo la responsabilidad del contratista en caso de terminación anticipada, definitiva, temporal o cesión del contrato.
c. La Oficina de Tecnologías de la Información debe parametrizar en el directorio activo, la inactivación automática de los contratistas, teniendo en cuenta la fecha de terminación del contrato; la inactivación de los usuarios de los sistemas de información que no se autentican con el directorio activo, se debe hacer de forma manual.
d. El Grupo Interno de Trabajo de Gestión del Talento y el Grupo Interno de Trabajo de Contratación o a quienes se deleguen deberán informar a la Oficina de Tecnologías de la Información a través de la Mesa de Servicios, cualquier novedad de desvinculación administrativa, laboral o contractual del colaborador; una vez notificada la novedad la Oficina de Tecnologías de la Información deberá proceder a la inactivación de los accesos del colaborador, teniendo en cuenta los siguientes parámetros:
    - Si el buzón pertenece a una cuenta de correo genérica (ejemplo: info@mintic.gov.co), a este se le deberá cambiar la contraseña inmediatamente y asignar nuevo responsable para evitar accesos no autorizados.
    - En caso de que el buzón sea objeto de investigación por parte de las autoridades competentes se les entregará en cadena de custodia una copia del buzón

garantizando su integridad. Se deben inactivar los accesos biométricos o de tarjetas de proximidad de los sistemas de control de acceso.

e. Para el buzón de correo electrónico se creará una copia de respaldo una vez se dé por terminada la vinculación con el Ministerio.
f. Bajo ningún parámetro se podrán restablecer los accesos a estas cuentas; solo se podrán restablecer buzones en ambientes offline y no se podrán emitir correos ni notificaciones desde estos buzones.
g. Se deben inactivar todos los accesos a los sistemas de información.
h. Se debe solicitar la devolución del carné o cualquier distintivo de autenticación o prenda de vestir, que lo acredita como colaborador del Ministerio.

7.3. LINEAMIENTOS DE SEGURIDAD PARA LA GESTIÓN DE ACTIVOS

Código: SI-A.8.1 – Responsabilidad por los Activos
Propósito: Establecer lineamientos para la identificación y valoración de los activos de información de la Entidad, y definir las responsabilidades para su protección.
Lineamientos:

a. La Subdirección Administrativa y de Gestión Humana del Ministerio de TIC, con el acompañamiento permanente de la Oficina de Tecnologías de la Información, deben diseñar una metodología para la identificación, clasificación, valoración y buen uso de los activos de información.
b. Todas las dependencias del Ministerio TIC deben contar con un inventario de sus activos de información y se debe evidenciar a través de los instrumentos dispuestos.
c. La Subdirección Administrativa y de Gestión Humana del Ministerio de TIC con acompañamiento de la Oficina de Tecnología de la Información y Oficina Asesora de Planeación y Estudios Sectoriales deben consolidar los inventarios reportados por los procesos en un instrumento único que contenga todos los activos de información del Ministerio.
d. La Oficina Asesora de Planeación y Estudios Sectoriales debe extraer del inventario de activos de información del Ministerio lo requerido para el reporte del índice de transparencia, de acuerdo con lo establecido en los instrumentos de gestión de la información adoptados mediante la Resolución 318 de febrero de 2018; para la publicación es necesario que cuente con la validación de la Oficina Asesora Jurídica en el marco de la clasificación de la información (Pública, Clasificada y reservada).
e. La Oficina de Tecnologías de la Información debe identificar los ciberactivos (activos de seguridad digital) críticos con base en los activos críticos definidos en el análisis de impacto en el negocio (BIA). Estos ciberactivos son aquellos que contienen, trasmiten o procesan información de los servicios esenciales de Ministerio.

f. Las firmas de documentos oficiales y que se constituye como activos de información de acuerdo a la tabla de retención documental o acto administrativo deben reposar en original o con firma digital del sistema de gestión documental, en ningún caso se debe utilizar firmas facsímil, digitalizadas o escaneadas, salvo en aquellos que se autorice por Resolución expedida por la Ministra de TIC, indicando para que fin y porque medios podrá ser utilizada.
g. Los servidores públicos y contratistas del Ministerio deben hacer entrega de los activos bajo su responsabilidad de acuerdo al formato de Paz y Salvo del Proceso de Gestión de Recursos Administrativos.

Código: SI-A.8.2 – Clasificación de la Información
Propósito: Establecer lineamientos para la protección de la información de la Entidad, de acuerdo con su criticidad.
Lineamientos:

a. La metodología de clasificación de información del Ministerio de que trata la Resolución de Seguridad y Privacidad de la Información, seguridad digital y continuidad del servicio, podrá integrarse con la metodología para la identificación, clasificación, valoración y buen uso de los activos de información, que trata el lineamiento en el código SI-A.8.1.
b. La Subdirección Administrativa y de Gestión Humana del Ministerio de TIC en conjunto con la Oficina de Tecnologías de la Información deben diseñar una guía para el rotulado de la información física y digital de acuerdo con lo establecido en la normatividad sobre información pública y protección de datos personales.
c. Las Tablas de Retención Documental (TRD) deben indicar el tipo de clasificación de las series, subseries y documentos en ella contenidas.
d. La Oficina de Tecnologías de la Información debe cumplir con los requerimientos de uso, manipulación y conservación de los medios tecnológicos para almacenamiento de información dadas por el fabricante, con el fin de mantener la disponibilidad e integridad de la información.
e. Los colaboradores deben aplicar la clasificación de la información del Ministerio, las TRD, el inventario de activos de información y la guía para la rotulación de la información.
f. Cada Propietario del activo de Información debe velar el cumplimiento de su clasificación de acuerdo con lo establecido en la guía para la rotulación de la información.
g. Para el intercambio de información se debe tener en cuenta su clasificación para su debida protección en términos de confidencialidad.

Código: SI-A.8.3 – Manejo de Medios
Propósito: Establecer lineamientos para evitar la divulgación, modificación, retiro o destrucción de la información almacenada en los medios de la Entidad.
Lineamientos:

a. La Oficina de Tecnologías de la Información debe definir un procedimiento para el uso de medios removibles.
b. La Oficina de Tecnologías de la Información debe proveer a los usuarios del Ministerio los métodos de cifrado de la información, así como administrar el software o herramienta utilizado para tal fin, y generar la guía para el usuario.
c. Todo medio removible deberá ser escaneado mediante el antivirus suministrado por la Oficina de Tecnologías de la Información cada vez que se conecte a un equipo del Ministerio.
d. Es responsabilidad de cada colaborador tomar las medidas para la protección de la información contenida en medios removibles, para evitar acceso físico y lógico no autorizado, daños, pérdida de información o extravío del mismo.
e. Se prohíbe el uso de medios removibles que contengan información reservada o clasificada del Ministerio en dispositivos de acceso al público.
f. La Subdirección Administrativa y de Gestión Humana del Ministerio de TIC debe crear o actualizar si fuere necesario el procedimiento o documento donde se establezca la disposición final de residuos de aparatos eléctricos y electrónicos (RAEE).
g. Se deberán emplear herramientas de borrado seguro y demás mecanismos de seguridad pertinentes en los medios de propiedad del Ministerio que serán reutilizados o eliminados, con el fin de controlar que la información del Ministerio contenida en estos medios no se pueda recuperar. Esta solicitud deberá ser mediante requerimiento a la Mesa de Servicios, con aprobación del jefe inmediato o supervisor de contrato.
h. Cuando se requiera transferir un medio de almacenamiento de información del Ministerio a otras entidades se deben establecer un acuerdo entre las partes. Dichos acuerdos deben dirigirse a la transferencia segura de información de interés entre el Ministerio y las partes.
i. Cuando se requiera transferir un medio de almacenamiento se debe tener en cuenta el registro de contenido de los medios, la protección aplicada, al igual que los tiempos de transferencia a los responsables durante el transporte y el recibido.
j. Los colaboradores y terceras partes que interactúen en procesos de intercambio de información al exterior del Ministerio deben cumplir los lineamientos, recomendaciones o estrategias establecidas por la Oficina de Tecnologías de la Información con el fin de garantizar su recuperación en caso de desastre.
k. El transporte para los medios de almacenamiento debe contar con las condiciones apropiadas para salvaguardar la integridad, confidencialidad y disponibilidad de la información del Ministerio.

7.4. LINEAMIENTOS DE SEGURIDAD PARA EL CONTROL DE ACCESO.

Código: SI-A.9.1 – Requisitos de la Entidad para el control de acceso.
Propósito: Establecer lineamientos para controlar el acceso a la información y las instalaciones de procesamiento de información de la Entidad.
Lineamientos:

a. La Oficina de Tecnologías de la Información debe suministrar a los usuarios las credenciales para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados; las credenciales de acceso son de uso personal e intransferible.
b. La conexión remota a la red de área local del Ministerio debe establecerse a través de una conexión VPN, la cual deberá ser aprobada, registrada y monitoreada por la Oficina de Tecnologías de la Información.
c. La Oficina de Tecnologías de la Información debe establecer una segregación de las redes, separando los entornos de red de usuarios de los entornos de red de servicios.
d. La Oficina de Tecnologías de la Información debe establecer para el control de acceso a los datos, información y servicios el principio del menor privilegio y la necesidad de conocer, lo que implica que no se otorgará acceso a menos que sea explícitamente autorizado.
e. La Oficina de Tecnologías de la Información debe verificar periódicamente los controles de acceso para los usuarios del Ministerio y los provistos a terceras partes, con el fin de revisar que dichos usuarios tengan los permisos únicamente a aquellos recursos de red y servicios de la plataforma tecnológica para los que fueron autorizados
f. La Oficina de Tecnologías de la Información debe revisar que los equipos personales de los colaboradores que se conecten a las redes de datos del Ministerio cumplan con todos los requisitos o controles para autenticarse y únicamente podrán realizar las tareas para las que fueron autorizados.

Código: SI-A.9.2 – Gestión de Acceso de Usuarios.
Propósito: Establecer lineamientos para prevenir el acceso no autorizado a sistemas y servicios de la Entidad.
Lineamientos:

a. La Oficina de Tecnologías de la Información debe definir un procedimiento para el registro y la cancelación de usuarios en el Ministerio, teniendo en cuenta que las identificaciones de los usuarios deberán ser únicas.
b. La Oficina de Tecnologías de la Información debe definir un estándar para la identificación de usuarios, teniendo en cuenta los siguientes parámetros:
    - Usar la primera letra del primer nombre más el apellido, en caso de homónimos se utiliza, la primera letra del primer nombre más la primera letra del segundo nombre más el apellido, de persistir la situación, se deberá utilizar la primera letra del primer nombre más el apellido, seguido de la primera letra del segundo apellido; si todas

las opciones anteriores se encuentra en uso, se utilizará la primera letra del primer nombre más la primera letra del segundo nombre más el primer apellido más la primera letra del segundo apellido.

c. El nombre para mostrar debe ser los nombres y apellidos completos. El usuario de correo electrónico debe ser igual al usuario de red, es decir debe existir interoperabilidad entre el servicio de correo y el directorio activo (DA).
d. La Oficina de Tecnologías de la Información solo otorgará a los usuarios accesos solicitados y autorizados por el jefe inmediato o supervisor del contrato.
e. Las cuentas de usuario por defecto de los sistemas operativos o aplicaciones tales como: “root”, “adm”, “admin”, “administrador”, “SQLAdmin”, “administrator” y “system”, entre otros, deben ser deshabilitadas siempre que no sean de uso obligatorio para el funcionamiento del servicio, de ser así, las credenciales de acceso deben ser asignadas, controladas, monitoreadas y vigiladas por los por los administradores de los servicios de la Oficina de Tecnologías de la Información, éstas deben cumplir con los parámetros definidos para el uso de contraseñas.
f. Solo se debe otorgar los privilegios para la administración de recursos tecnológicos, servicios de red, sistema operativo y sistemas de información únicamente a aquellos colaboradores que cumplan dichas funciones, deben ser cuentas únicas asociadas al usuario de dominio del colaborador; en caso de requerirse usuarios de acceso genérico, éstos deben ser entregados al colaborador de manera formal por parte del jefe inmediato o supervisor del contrato; en caso de cambiar el titular de la cuenta genérica las credenciales de acceso deben ser modificadas me manera inmediata.
g. Deberá restringir las conexiones remotas para la administración de la plataforma tecnológica; únicamente se deberá permitir el acceso a los colaboradores autorizados por la Oficina de Tecnología de la Información.
h. La Oficina de Tecnología de la Información debe deshabilitar los servicios o funcionalidades no utilizadas de los sistemas operativos, el firmware y las bases de datos.
i. La Oficina de Tecnologías de la Información debe mantener un listado actualizado con las cuentas que administren todos los recursos tecnológicos.
j. La contraseña para la autenticación se debe suministrar a los usuarios de manera segura, y el sistema debe solicitar el cambio inmediato de la misma al ingresar.
k. Se debe establecer procedimientos para verificar la identidad de un usuario antes de reemplazar la información secreta para la autenticación o proporcionar una nueva o temporal.
l. La Oficina de Tecnologías de la Información debe generar reportes de uso de cada uno de los sistemas de información o recursos tecnológicos con el fin de identificar la periodicidad de uso de los usuarios, en caso de identificar inactividad mayor a 15 días se bloqueará el usuario y se debe realizar validación con el área a la que pertenece para determinar si se procede a la deshabilitación definitiva o temporal por novedad.

m. La Oficina de Tecnologías de la Información debe revisar los derechos de acceso de los usuarios administradores por lo menos dos veces al año.
n. Para realizar el ajuste o retiro de los derechos de acceso se debe tener en cuenta lo establecido en el control SI-A.7.3 de este documento.

Código: SI-A.9.3 – Responsabilidades de los Usuarios.
Propósito: Establecer lineamientos para que los usuarios salvaguarden sus credenciales de acceso a los servicios de la Entidad.
Lineamientos:

a. El cambio de contraseña solo podrá ser solicitada por el titular de la cuenta, su jefe inmediato o supervisor del contrato.
b. Las contraseñas deben poseer algún grado de complejidad y no deberán ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, por ejemplo: fechas de cumpleaños, nombre de los hijos, placas de automóvil, etc.
c. La contraseña debe cumplir con las siguientes recomendaciones como mínimo:
    - Deberá tener como mínimo ocho (8) caracteres alfanuméricos sin repetición.
    - No debe contener el nombre de usuario, el nombre real o las siglas MINTIC, FONTIC, TIC.
    - No se deben usar contraseñas con los nombres de los hijos, esposo, mascotas, fechas de aniversarios, cumpleaños, etc.
    - Deben ser diferentes de otras contraseñas anteriores proporcionadas, es decir las ultimas diez (3) suministradas al dominio no se deberán repetir.
    - No se deberán usar las mismas contraseñas de la autenticación para uso personal.
    - Deben estar compuestas por: letras en mayúsculas “A, B, C…”, letras en minúsculas “a, b, c…”, números “0, 1, 2, 3…”, símbolos especiales “@, #, $, %, &, (), ¡, !, ¿, ?, <>…” en cualquier combinación.
    - Debe cambiarse obligatoriamente cada 90 días.
    - Después de 3 (tres) intentos no exitosos de ingreso de la contraseña el usuario deberá ser bloqueado de manera inmediata y deberá esperar un tiempo determinado de 2 minutos para volver a intentar, o solicitar el desbloqueo a través de la Mesa de Servicios.
    - Debe cambiarse si se ha detectado anomalía en la cuenta de usuario.
    - Debe no ser visible en la pantalla, al momento de ser ingresada.
    - No se debe registrar en papel, correo electrónico, archivos digitales a menos que se puedan almacenar de forma segura y el método de almacenamiento esté aprobado por la Oficina de Tecnologías de la Información.

Código: SI-A.9.4 – Control de Acceso a Sistemas y Aplicaciones.
Propósito: Establecer lineamientos prevenir el acceso no autorizado a sistemas y aplicaciones y servicios de la Entidad.
Lineamientos:

a. La Oficina de Tecnologías de la Información debe implementar controles para que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción, y así mismo que los menús muestren los mensajes de identificación apropiados para reducir los riesgos de error.
b. La Oficina de Tecnologías de la Información debe establecer el procedimiento y los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, debe implementar para los desarrolladores internos o externos acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.
c. El uso de programas que puedan ser capaces de invalidar los controles del sistema y de la aplicación, deben estar restringidos y estrictamente controlados.
d. Las sesiones inactivas deben cerrarse después de un período de inactividad definido de 3 minutos y se deben usar restricciones en los tiempos de conexión para proporcionar una seguridad adicional a las aplicaciones de alto riesgo.
e. La Oficina de Tecnologías de la Información debe integrar la autenticación de las aplicaciones con el Directorio Activo.
f. La Oficina de Tecnologías de la Información debe establecer los controles para que los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información, no tengan instalados en sus equipos de cómputo programas utilitarios que permitan escalar privilegios o evadir controles de seguridad informáticos sin ser debidamente autorizados.
g. La Oficina de Tecnologías de la Información debe monitorear a los administradores de los recursos tecnológicos y servicios de red, para que no hagan uso de programas utilitarios que permitan acceso a los sistemas operativos, firmware o conexión a las bases de datos para anular la seguridad de los sistemas de información alojados sobre la plataforma tecnológica.
h. La Oficina de Tecnologías de la Información debe generar y mantener actualizado un listado de programas utilitarios privilegiados de la plataforma tecnológica, los servicios de red y sistemas de información autorizados.
i. La Oficina de Tecnologías de la Información debe retirar o deshabilitar los programas utilitarios privilegiados no autorizados de la plataforma tecnológica, los servicios de red y sistemas de información y bloquear su conexión a través de los servicios perimetrales e internos de seguridad informática.
j. El acceso al código fuente del programa es limitado, solamente los ingenieros desarrolladores y de soporte autorizados de la Oficina de Tecnologías de la Información.
k. Las librerías de los sistemas de información no deberán estar contenidas en el ambiente de producción.

7.5. LINEAMIENTOS DE SEGURIDAD PARA EL USO DE RECURSOS CRIPTOGRÁFICOS.

Código: SI-A.10.1 – Controles Criptográficos.
Propósito: Establecer lineamientos para el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad e integridad de la información de la Entidad.
Lineamientos:

a. La Oficina de Tecnologías de la Información debe establecer gestionar los controles criptográficos en los siguientes casos:
   - Para la protección de claves de acceso a sistemas, datos y servicios.
   - Para la información digital reservada y clasificada.
   - Para el envió de correo electrónico con información reservada y clasificada.

b. La Oficina de Tecnologías de la Información debe verificar que todo sistema de información que requiera realizar transmisión de información clasificada o reservada cuente con mecanismos de cifrado de datos.
c. La Oficina de Tecnologías de la Información debe desarrollar, establecer e implementar estándares para la aplicación de controles criptográficos en los servicios que lo requieran.
d. La Oficina de Tecnologías de la Información debe utilizar controles criptográficos para la transmisión de información clasificada o reservada, fuera del ámbito del Ministerio.
e. La Oficina de Tecnologías de la Información en cabeza de los proveedores de desarrollado de software deben asegurar que los controles criptográficos de los sistemas construidos cumplen con los estándares establecidos por el Ministerio.
f. La Oficina de Tecnologías de la Información debe disponer de herramientas que permitan el cifrado de medios de almacenamiento de información.

7.6. LINEAMIENTOS DE SEGURIDAD FÍSICA Y DEL ENTORNO

Código: SI-A.11.1 – Áreas Seguras.
Propósito: Establecer lineamientos para prevenir el acceso físico no autorizado, el daño e interferencia de la información e instalaciones de procesamiento de información de la Entidad.
Lineamientos:

a. La Subdirección Administrativa y de Gestión Humana debe señalizar las áreas seguras de acuerdo al inventario de áreas seguras.
b. Las puertas y ventanas de las áreas seguras deberán permanecer cerradas con llave cuando no hay supervisión o están desocupadas.
c. Todos los puntos de acceso deberán tener un área de recepción con vigilancia u otro medio para controlar el acceso físico al sitio o instalación.
d. El perímetro de seguridad de las áreas seguras debe contar con vigilancia mediante CCTV y debe ser monitoreado por el personal de vigilancia del Ministerio.

e. La Subdirección Administrativa y de Gestión Humana debe establecer un sistema de control de acceso a las instalaciones del Ministerio, así como a las áreas seguras y se debe documentar mediante un procedimiento, manual o guía.
f. El personal de vigilancia debe establecer mecanismos para inspeccionar y examinar los morrales, bolsos, cajas, etc. que ingresen los colaboradores o visitantes.
g. El personal de vigilancia debe registra en una bitácora o sistema de información el ingreso y retiro de todo equipo cómputo (pc o portátil, mouse, teclado, cargador, etc.), servidores, equipos activos de red o cualquier equipo electrónico diferentes a smartphone; en caso de que estos equipos sean propiedad del Ministerio deberán contar con autorización expresa de la Subdirección Administrativa y de Gestión Humana u Oficina de Tecnologías de la Información según sea el caso y de acuerdo a los procedimientos establecidos para tal fin.
h. La Oficina de Tecnologías de la Información y la Subdirección Administrativa y de Gestión Humana deben controlar el ingreso a los centros de datos y centros de cableado del Ministerio.
i. La Oficina de Tecnologías de la Información y la Subdirección Administrativa y de Gestión Humana autorizan el ingreso a personal ajeno al Ministerio a los centros de datos y centros de cableado, este deberá estar acompañado por quien sea autorizado, éste se hará responsable de la estadía del personal ajeno al Ministerio durante el tiempo que permanezca en las instalaciones.
j. Todo el personal que ingrese al Centro de Datos y centros de cableado deberá portar identificación visible y presentarla en la puerta de acceso antes de su ingreso.
k. La Subdirección Administrativa y de Gestión Humana con acompañamiento de la Oficina de Tecnologías de la Información es responsable de la identificación y organización del cableado estructurado desde los puestos de trabajo hasta los paneles de conexión (patch panel) de los centros de cableado.
l. La Subdirección Administrativa y de Gestión Humana debe mantener en buen estado la infraestructura física de los centros de cableado y centros de datos del Ministerio, tales como puertas, cerraduras, ventanas, techos, paredes, pisos, aires acondicionados, cielos rasos, pisos falsos, sensores, entre otros.
m. La Oficina de Control Interno deben realizar una revisión periódica del estado de los centros de cableado e informar cualquier anomalía presentada de la siguiente manera: daños en el rack y equipos activos de red a la Oficina de Tecnologías de la Información, y daños en infraestructura física (puertas, cerraduras, ventanas, techos, paredes, pisos, aires acondicionados, cielos rasos, pisos falsos, entre otros) a la la Subdirección Administrativa y de Gestión Humana.
n. La Subdirección Administrativa y de Gestión Humana, son los responsables del cumplimiento del protocolo de aseo en los centros de cableado y centro de datos, este último contará con el acompañamiento de la Oficina de Tecnologías de la Información.

o. La Oficina de Tecnologías de la Información es responsable de mantener organizado e identificado el cableado en los racks de los centros cableado y centro de datos.
p. Se deberá establecer un plan de mantenimiento para los centros de cableado por parte de la la Subdirección Administrativa y de Gestión Humana y la Oficina de Tecnologías de la Información, de tal manera que se corrijan fallas y/o establecer mejoras en los mismos.
q. la Subdirección Administrativa y de Gestión Humana debe respaldar los videos generados por las cámaras de vigilancia e información generada de los accesos a las instalaciones del Ministerio de acuerdo a las políticas de respaldo de la información.
r. La Oficina de Tecnologías de la Información y la Subdirección Administrativa y de Gestión Humana, deben mantener libre de objetos o elementos que no sean propios en la operación en el centro de datos y centros de cableado del Ministerio.
s. La Subdirección Administrativa y de Gestión Humana en acompañamiento de la Subdirección Financiera debe establecer mecanismos de seguridad para el ingreso a las áreas de procesamiento de pagos y debe ser monitoreado mediante circuito cerrado de televisión (CCTV), que cubra el acceso al área y al funcionario que utilice los equipos financieros, en ningún caso deberá grabarse o monitorear directamente la pantalla o el teclado de los equipos financieros.
t. El Oficial de Seguridad de la Información, la Oficina de Tecnologías de la Información y la Subdirección financiera deben desarrollar la Guía de Seguridad para el manejo y control de los recursos financieros administrados por el Ministerio.
u. La Subdirección Administrativa y de Gestión Humana con el apoyo de la Oficina de Tecnologías de la Información establecerán los lineamientos para los controles contra amenazas externas y ambientales y quedarán enmarcadas en los planes de contingencia, de emergencia y de continuidad del negocio.
v. En las áreas seguras se debe restringir el uso de equipo fotográfico, de video, audio u otro equipo de grabación, tales como cámaras en dispositivos móviles, a menos que se cuente con autorización para ello por parte del área encargada, está prohibición debe estar señalizada.
w. El trabajo en áreas seguras debe estar monitoreado por CCTV, teniendo en cuenta que las cámaras no podrán apuntar directamente a la captura de información dentro de estas áreas.
x. Se prohíbe el consumo de alimentos y bebidas en las áreas seguras del Ministerio, esta prohibición debe ser señalizada.
y. La Subdirección Administrativa y de Gestión Humana debe señalizar las áreas de cargue y descargue del Ministerio.
z. Los puntos de acceso como el área de entrega y las zonas de carga deberán ser controladas y monitoreadas mediante CCTV.
aa. El personal de vigilancia con el acompañamiento de la Subdirección Administrativa y de Gestión Humana debe inspeccionar y examinar el material que ingresa por las áreas de cargue para determinar la presencia de materiales peligrosos.

Código: SI-A.11.2 – Equipos.
Propósito: Establecer lineamientos para prevenir perdida, daños, robo o compromisos de activos y la interrupción de las operaciones de la Entidad.
Lineamientos:

a. La Subdirección Administrativa y de Gestión Humana con el apoyo de la Oficina de Tecnologías de la Información propenderán que los equipos de cómputo e impresoras estén situados y protegidos en áreas para reducir el riesgo contra amenazas ambientales y de acceso no autorizado.
b. La Oficina de Tecnología de la Información debe propender que los equipos de cómputo portátiles suministrados por la Entidad se protejan mediante mecanismos que no permitan su pérdida.
c. La Subdirección Administrativa y de Gestión Humana con el apoyo de la Oficina de Tecnologías de la Información establece los lineamientos para el uso de la red de energía regulada en los puestos de trabajo en los cuales solo se deben conectar equipos como computadores de escritorio, portátiles y pantallas; los otros elementos deben conectarse a la red eléctrica no regulada.
d. La Subdirección Administrativa y de Gestión Humana con el apoyo de la Oficina de Tecnologías de la Información deben implementar mecanismos para regular el flujo de energía e interrupciones causadas por fallas en el soporte de los servicios públicos que puedan afectar los equipos de cómputo y procesamiento de información.
e. Para propender por la continuidad de los servicios y la operación del Ministerio en caso de fallas en el fluido eléctrico externo, la Subdirección Administrativa y de Gestión Humana debe suministrar una planta eléctrica y la Oficina de Tecnologías de la Información las UPS necesarias, y garantizar su manteamiento preventivo y correctivo.
f. La Subdirección Administrativa y de Gestión Humana debe proteger el cableado que transporta voz, datos y suministro de energía eléctrica contra la interceptación, interferencia o daños de cualquier tipo dentro del perímetro del Ministerio.
g. Los cables de energía eléctrica deberán estar separados de los cables de comunicaciones para evitar interferencia y ruido.
h. Al momento de instalar o actualizar el cableado estructurado se debe tener en cuenta las consideraciones técnicas de las normas vigentes y el Reglamento Técnico de Instalaciones Eléctricas RETIE.
i. Los cuartos de cableado solo podrán tener los elementos activos para su funcionamiento y no utilizarse como almacén para guardar cajas, mesas u otros equipos que no estén en uso.
j. La Oficina de Tecnologías de la Información bebe definir mecanismos de soporte y mantenimiento a los equipos de cómputo, servidores y equipos activos de red y debe llevar registro de estos.

k. Solo el personal autorizado por la Oficina de Tecnologías de la información puede llevar a cabo el mantenimiento o las reparaciones a los equipos de cómputo, servidores o activos de red.
l. Las actividades de mantenimiento de los servidores, elementos de comunicaciones, energía o cualquiera que pueda ocasionar una suspensión en el servicio, deberán ser programadas por la Oficina de Tecnologías de la información.
m. En los casos en que los equipos requieran salir de las instalaciones del Ministerio para reparación, mantenimiento o cambio, la Oficina de Tecnologías de la información debe verificar que en estos no se encuentre información Clasificada o Reservada, en dicho caso se debe realizar respaldo de la información y un borrado seguro.
n. Cuando un equipo o medio extraíble sea reasignado o retirado de servicio, la Oficina de Tecnologías de la Información debe garantizar la eliminación de toda información mediante mecanismos de borrado seguro teniendo en cuenta que previo a esta actividad debe realizarse una copia de seguridad de la misma; en caso de dar de baja para disposición final y no para subastar, se debe tener en cuenta lo establecido en el SI-A.8.3 – Manejo de Medios literal f.
o. Para el retiro de activos de las instalaciones del Ministerio se debe tener en cuenta lo establecido en el control SI-A.11.1 – Áreas Seguras literal g del presente documento.
p. Para el retiro de activos del almacén, la Subdirección Administrativa y de Gestión Humana deberá llevar un control en el aplicativo de inventarios con el fin de mantener registro de asignación y devolución.
q. Para mantener la seguridad de la información en los equipos y activos fuera de las instalaciones del Ministerio y que contengan información clasificada o reservada, estos deben contar con lo establecido en el SI-A.10.1 – Controles Criptográfico literal f.
r. Los Colaboradores del Ministerio, durante su ausencia no deberán conservar sobre el escritorio información propia del Ministerio como: documentos físicos o medios de almacenamiento, por lo tanto, se requiere guardar en un lugar seguro para impedir su pérdida, daño, copia o acceso por parte terceros o personal que no tenga autorización para su uso o conocimiento.
s. Los Colaboradores del Ministerio, deben bloquear la pantalla del computador a su cargo cuando se ausenten de su puesto de trabajo, para impedir el acceso de terceros no autorizados a la información almacenada en el equipo de cómputo.
t. Los Colaboradores del Ministerio que impriman documentos con clasificación (Clasificada – Reservada), estos deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.
u. No se debe reutilizar documentos impresos con clasificación (Clasificada – Reservada), estos deben ser destruidos y no deben estar como papel reciclable.
v. Los puestos de trabajo de los Colaboradores del Ministerio y terceras partes que prestan sus servicios y cuyas funciones no obliguen a la atención directa de ciudadanos deberán

localizarse preferiblemente en ubicaciones físicas que no estén expuestas al público para minimizar los riesgos asociados al acceso no autorizado de la información o a los equipos informáticos.

w. La Oficina de Tecnologías de la Información debe configurar como política general que todos los equipos de cómputo que se encuentren en los dominios del Ministerio bloqueen automáticamente su sesión después de tres (3) minutos de inactividad.

x. La Oficina de Tecnologías de la Información debe configurar como política general que todos los equipos de cómputo que se encuentren en los dominios del Ministerio oculten de manera automáticas los iconos, accesos directos o documentos que se encuentren en el escritorio.

7.7. LINEAMIENTOS DE SEGURIDAD DE LAS OPERACIONES

Código: SI-A.12.1 – Procedimientos operacionales y responsabilidades.
Propósito: Establecer lineamientos para asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información de la Entidad.
Lineamientos:

a. La Oficina de Tecnologías de la Información con el apoyo de la Oficina Asesora de Planeación y Estudios Sectoriales debe documentar y mantener actualizados todos sus procedimientos operativos para garantizar la disponibilidad, integridad y confidencialidad de la información.

b. La Oficina de Tecnologías de la Información debe poner a disposición de todos los colaboradores los procedimientos de operación mediante los medios que el Ministerio disponga.

c. La Oficina de Tecnologías de la Información debe establecer un procedimiento que permita asegurar la gestión de cambios normales y de emergencia a nivel de infraestructura, aplicativos y servicios tecnológicos para que estos sean desarrollados bajo estándares de eficiencia, seguridad, calidad y permitan determinar las actividades y responsables en la gestión de cambios.

d. La Oficina de Tecnologías de la Información debe establecer el comité de cambios normales y el de emergencia, quien se encargará de evaluar, aprobar o negar la implementación de los cambios y este a su vez será presidido por el Gestor de Cambios.

e. La Oficina de Tecnologías de la Información debe establecer una guía o manual de operación de gestión de cambios normales y de emergencia que contenga el detalle operativo del proceso de cambios.

f. La Oficina de Tecnologías de la Información debe documentar la gestión de capacidad de la plataforma tecnológica, definir su responsable y mantenerla actualizada, la cual permita:

   - Evaluar las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad.

- Monitorear el rendimiento de la infraestructura tecnológica para determinar el uso de la capacidad existente.
- Documentar los datos de rendimiento y capacidad de la plataforma tecnológica del Ministerio.
- Documentar los acuerdos de niveles de servicio.
- Asignar los recursos adecuados de hardware y software, para todos los servicios y aplicaciones de tecnología.

g. La Oficina de Tecnologías de la Información debe documentar las recomendaciones de mejora de la infraestructura de tecnología.
h. La Oficina de Tecnologías de la Información debe definir los indicadores de rendimiento correspondientes a la gestión de capacidad de la plataforma tecnológica.
i. La Oficina de Tecnologías de la Información debe propender por la separación de los ambientes de desarrollo, pruebas y producción, los cuales deben estar separados de manera física y lógica.
j. La Oficina de Tecnologías de la Información debe definir, documentar y aplicar lineamientos seguros para la transferencia entre ambientes.
k. La Oficina de Tecnologías de la Información debe utilizar en los ambientes de prueba datos que no sean sensibles para el Ministerio.
l. La Oficina de Tecnologías de la Información debe permitir que los ambientes de prueba, desarrollo y producción sean similares para prevenir situaciones en las cuales el software desarrollado presente comportamientos distintos y errores.
m. La Oficina de Tecnologías de la Información debe utilizar nombres de dominios diferentes para los ambientes de prueba, desarrollo y producción para evitar confusión y diferenciar de manera clara cada ambiente.
n. La Oficina de Tecnologías de la Información debe garantizar que los desarrolladores realicen su trabajo exclusivamente en el ambiente de desarrollo y nunca en los ambientes de pruebas o producción.

Código: SI-A.12.2 – Protección contra códigos maliciosos.
Propósito: Establecer lineamientos para asegurar que la información y las instalaciones de procesamiento de información de la Entidad estén protegidas contra códigos maliciosos.
Lineamientos:

a. La Oficina de Tecnologías de la Información debe definir y documentar los controles para la detección, prevención y recuperación contra códigos maliciosos.
b. La Oficina de Tecnologías de la Información con el apoyo del Oficial de Seguridad de la Información deben realizar campañas de concienciación de usuarios en materia de protección, prevención y recuperación contra códigos maliciosos.
c. La Oficina de Tecnologías de la Información debe mantener actualizada la base de datos, base de firmas y parches correspondiente del del software antivirus y debe asegurar que esta herramienta no pueda ser deshabilitada de los equipos del Ministerio.

d. La Oficina de Tecnologías de la Información debe dictar los lineamientos para la instalación del software antivirus con el fin de brindar protección contra códigos maliciosos en todos los recursos informáticos del Ministerio.
e. La Oficina de Tecnologías de la Información debe aplicar las actualizaciones y parches de seguridad de los sistemas operativos de los equipos y servidores del Ministerio para protegerlos contra códigos maliciosos.
f. Todo mensaje sospechoso de procedencia desconocida debe ser inmediatamente reportado a la Oficina de Tecnologías de la Información a través de la Mesa de Servicios, tomando las medidas de control necesarias.

Código: SI-A.12.3 – Copias de respaldo.
Propósito: Establecer lineamientos para proteger la información de la Entidad contra la pérdida de datos.
Lineamientos:

a. La Oficina de Tecnologías de la Información debe definir y documentar un plan o procedimiento de copias de respaldo y restauración de la información del Ministerio, donde se establezca el esquema, de qué, cómo, quién, con qué periodicidad, tipo de respaldo y nivel de criticidad.
b. La Oficina de Tecnologías de la Información debe definir y documentar lineamientos para la realización de copias de respaldo de:
    - Bases de datos de producción.
    - Software de aplicaciones.
    - Sistemas operativos.
    - Configuraciones de servidores.
    - Software base del Ministerio.
c. La Oficina de Tecnologías de la Información debe realizar y mantener las copias de respaldo de la información digital solicitadas.
d. Oficina de Tecnologías de la Información debe disponer de herramientas tecnológicas para gestionar la información digital del Ministerio y asegurar que estas dispongan de copias de respaldo.
e. La Oficina de Tecnologías de la Información debe definir la custodia y almacenamiento de las copias de respaldo.
f. La Oficina de Tecnologías de la Información debe tener un inventario y bitácora de las copias de respaldo que se realizan y de las copias de respaldo que se restauran.
g. La Oficina de Tecnologías de la Información debe generar mecanismos que mantengan la integridad y confidencialidad de las copias de respaldo.
h. Los colaboradores deben utilizar las herramientas tecnológicas dispuesta por la Oficina de Tecnologías de la Información para gestionar la información del Ministerio.

i. Los colaboradores son responsables de la información que resida en el equipo asignado y serán los encargados de mantener copias de respaldo de sus archivos, y la información debe ser entregada al supervisor del contrato o jefe inmediato al finalizar su vinculación con el Ministerio. En caso de que los colaboradores requieran la ejecución de una copia de respaldo de su información, lo pueden solicitar a la Oficina de Tecnologías de la Información a través de la Mesa de Servicios.

Código: SI-A.12.4 – Registro y seguimiento.
Propósito: Establecer lineamientos para registrar los eventos de seguridad de la información de la Entidad y generar las evidencias.
Lineamientos:

a. La Oficina de Tecnologías de la Información debe generar registros de auditoría que contengan excepciones o eventos relacionados a la seguridad en los sistemas de información que se consideren.
b. La Oficina de Tecnologías de la Información debe salvaguardar los registros de auditoría que se generen de cada sistema.
c. La Oficina de Tecnologías de la Información debe monitorear excepciones o los eventos de la seguridad de información.
d. La Oficina de Tecnologías de la Información debe monitorear la infraestructura tecnológica para verificar que los usuarios sólo la usen para actividades propias de su labor y la Misión del Ministerio.
e. La Oficina de Tecnologías de la Información debe sincronizar los relojes de los servidores con una única fuente de referencia de tiempo (http://horalegal.inm.gov.co/), con el fin de garantizar la exactitud de los registros de auditoría.

Código: SI-A.12.5 – Control de software operacional.
Propósito: Establecer lineamientos para asegurar la integridad de los sistemas operacionales de la Entidad.
Lineamientos:

a. La Oficina de Tecnologías de la Información debe controlar y tener registros de la actualización del software en producción, aplicaciones y librerías de programas propios del Ministerio.
b. La Oficina de Tecnologías de la Información debe conservar las versiones anteriores del software de aplicación como una medida de contingencia.
c. La Oficina de Tecnologías de la Información debe usar controles para proteger todo el software implementado y la documentación del sistema.

Código: SI-A.12.6 – Gestión de la vulnerabilidad técnica.
Propósito: Establecer lineamientos para prevenir la explotación de las vulnerabilidades técnicas de la Entidad.
Lineamientos:

a. La Oficina de Tecnologías de la Información debe realizar mínimo una vez al año una revisión de vulnerabilidades técnicas a los sistemas de información críticos y misionales por medio de ethical hacking y/o pruebas de penetración.
b. La Oficina de Tecnologías de la Información debe documentar, informar, gestionar y corregir las vulnerabilidades encontradas, adoptando acciones correctivas para mitigar los hallazgos, minimizar el nivel de riesgo y reducir el impacto.
c. La Oficina de Tecnologías de la Información debe definir y establecer los roles y responsabilidades asociados con la gestión de la vulnerabilidad técnica, incluido el seguimiento de la vulnerabilidad, la valoración de riesgos de vulnerabilidad, las pruebas de gestión, la aplicación de parches, el seguimiento de activos y cualquier responsabilidad de coordinación requerida.
d. La Oficina de Tecnologías de la Información debe probar y evaluar la aplicación de actualizaciones antes de su instalación y valorar los riesgos asociados, para asegurar que son eficaces y no producen efectos secundarios.
e. La Oficina de Tecnologías de la Información debe restringir a los usuarios finales la instalación de software en los equipos del Ministerio.
f. La Oficina de Tecnologías de la Información debe establecer y monitorear que la infraestructura tecnológica sea usada exclusivamente para el desempeño laboral, o para el desarrollo de las funciones, actividades y obligaciones acordadas o contratadas.
g. La Oficina de Tecnologías de la Información debe controlar la instalación y uso de máquinas virtuales y sólo podrá realizarse siempre y cuando sea una necesidad para el uso de las funciones o labor contratada y no viole los derechos de autor.
h. La Oficina de Tecnologías de la Información debe realizar de manera periódica una inspección del software instalado en los equipos del Ministerio y debe desinstalar el software no autorizado.
i. La Oficina de Tecnologías de la Información a través de la Mesa de Servicios es la responsable de instalar, configurar y dar soporte a los equipos del Ministerio.
j. Sólo está permitido el uso de software licenciado por el Ministerio y/o aquel que sin requerir licencia de uso comercial sea expresamente autorizado por la Oficina de Tecnologías de la Información.
k. Las aplicaciones generadas por el Ministerio en desarrollo de su misión institucional deben ser reportadas a la Oficina de Tecnologías de la Información para su administración.
l. La Oficina de Tecnologías de la Información es la única dependencia autorizada para la administración del software, el cual no debe ser copiado, suministrado a terceros o utilizado para fines personales y comerciales.

Código: SI-A.12.7 – Consideraciones sobre auditorias de sistemas de información.
Propósito: Establecer lineamientos minimizar el impacto de las actividades de auditoria sobre los sistemas operativos de la Entidad.
Lineamientos:

a. La Oficina de Tecnologías de la Información debe planificar periódicamente actividades que involucren auditorias de los sistemas críticos en producción, limitando el acceso al sistema de información y a los datos de solo de lectura (en caso de acceso diferente al de solo lectura se deberá acordar previamente), determinando tareas, responsables y estas se deberán realizar fuera del horario laboral.
b. La Oficina de Tecnologías de la Información debe mantener los documentos, dispositivos y medios utilizados para las auditorias de los Sistemas de Información custodiados de accesos no autorizados.
c. La Oficina de Tecnologías de la Información debe documentar los resultados de las auditorias de los sistemas de Información del Ministerio.

7.8. LINEAMIENTOS DE SEGURIDAD DE LAS COMUNICACIONES

Código: SI-A.13.1 – Gestión de la seguridad de las redes.
Propósito: Establecer lineamientos para asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte de la Entidad.
Lineamientos:

a. La Oficina de Tecnologías de la Información debe proporcionar una plataforma Tecnológica que soporte los sistemas de información, esta debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a internet. La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad.
b. La Oficina de Tecnologías de la Información debe realizar segmentación de Redes para Colaboradores y visitantes del Ministerio.
c. La Oficina de Tecnologías de la Información debe establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.
d. La Oficina de Tecnologías de la Información es la responsable de garantizar que los puertos físicos y lógicos de diagnósticos y configuración de plataformas que soporten sistemas de información deban estar siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.

e. La Oficina de Tecnologías de la Información debe establecer la documentación necesaria para la utilización de los servicios de red restringiendo el acceso a los servicios de red y a las aplicaciones.
f. La Oficina de Tecnologías de la Información debe realizar revisiones y monitoreo regularmente a la gestión de los servicios para validar que se encuentran en los acuerdos de servicios de red establecidos con los proveedores.
g. La Oficina de Tecnologías de la Información debe definir controles para la transferencia de información a través de redes públicas para las aplicaciones del Ministerio.
h. La Oficina de Tecnologías de la Información debe disponer de controles para realizar transferencias completas, sin alteraciones y visualizaciones no autorizadas de la información entre las aplicaciones del Ministerio, teniendo en cuenta los siguientes criterios:
    - Contar con información de autenticación secreta de usuario.
    - Cifrar las comunicaciones entre DMZ y los servidores de la red interna.
    - Los protocolos de comunicación entre la red interna y la DMZ estén asegurados con el fin de prevenir fugas de información.
    - La información almacenada de las transacciones no se encuentre pública.
i. La Oficina de Tecnologías de la Información debe disponer de una zona desmilitarizada o DMZ, entre la red interna del Ministerio y la red externa (internet) con el objetivo de delimitar conexiones desde la red interna hacia Internet y limitar las conexiones desde internet hacia la red interna del Ministerio con los siguientes criterios:
    - EL tráfico de la red externa a la DMZ está limitado
    - El tráfico de la red externa a la red interna está prohibido
    - El tráfico de la red interna a la DMZ está limitado
    - El tráfico de la red interna a la red externa está autorizado
    - El tráfico de la DMZ a la red interna está prohibido
    - El tráfico de la DMZ a la red externa está denegado
j. La DMZ se debe implementar para ofrecer servicios que necesitan acceso desde internet. Estos servicios deberán ser monitoreados con el fin de prevenir ataques.
k. La arquitectura de la DMZ debe estar aislada de la red interna del Ministerio de forma que no permita el acceso no autorizado a la red interna, por lo que se deben diseñar redes perimetrales con los siguientes objetivos:
    - No se pueden hacer consultas directas a la red interna del Ministerio desde redes externas e internet.
    - Se deberá realizar la segmentación de redes y listas de acceso a los servicios del Ministerio tales como servidores, administración, invitados, Etc.
l. El acceso a la red de datos del Ministerio y a los sistemas de información soportados por la misma, es de carácter restringido. Se deben conceder permisos con base a “la necesidad de conocer” y el “acceso mínimo requerido” conforme a los criterios de seguridad de la información contemplados en la presente política.

Código: SI-A.13.2 – Transferencia de Información.
Propósito: Establecer lineamientos para mantener la seguridad de la información transferida dentro del Ministerio y con cualquier entidad externa.
Lineamientos:

a. La Oficina de Tecnologías de la Información debe contar con los lineamientos para proteger la información transferida con respecto a la interceptación, copiado, modificación, enrutado y destrucción de la misma.
b. La Oficina de Tecnologías de la Información debe establecer procedimientos para la detección de software malicioso y protección contra éste, que puede ser transmitido mediante el uso de comunicaciones electrónicas.
c. La Oficina de Tecnologías de la Información debe establecer controles para proteger la información que se transmite como documentos adjuntos a través del correo electrónico del Ministerio.
d. La Subdirección Administrativa y de Gestión Humana debe dictar directrices sobre retención, disposición y transferencia de la información física del Ministerio, de acuerdo con la legislación y reglamentaciones local y nacional aplicable.
e. La Oficina de Tecnologías de la Información debe establecer un acuerdo para la transferencia de información entre el Ministerio y las partes externas.
f. La Oficina de Tecnologías de la Información debe definir una Guía de Recolección de Evidencias de Elementos Informáticos, con el fin de garantizar la autenticidad de los elementos materiales de prueba recolectados y examinados, asegurando que pertenecen al caso investigado, sin confusión, adulteración o sustracción.
g. La Oficina de Tecnologías de la Información debe establecer los procedimientos para el direccionamiento y transporte correctos del mensaje, así como la confiabilidad y disponibilidad del servicio.
h. La Oficina de Tecnologías de la Información debe proporcionar herramientas de mensajería electrónica corporativas, como mensajería instantánea, redes sociales etc.
i. Para los acuerdos de confidencialidad y de no divulgación se debe tener en cuenta lo establecido en el control SI-A.7.1 literal e de este documento.
j. Para el personal externo que ejecute tareas propias del Ministerio y haya sido contratado en el marco de un contrato o convenio con el Ministerio, debe firmar un acuerdo de confidencialidad y no divulgación de la información firmado entre el Ministerio (Supervisor del Contrato) y el Representante Legal, y este debe reposar en la carpeta de ejecución del contrato.

7.9. LINEAMIENTOS DE SEGURIDAD PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Código: SI-A.14.1 – Requisitos de seguridad de los sistemas de información.
Propósito: Establecer lineamientos para promover que la seguridad de la información haga parte integral de los sistemas de información durante todo su ciclo de vida.
Lineamientos:

a. La Oficina de Tecnologías de la Información debe disponer de requerimientos para las solicitudes de nuevos Sistemas de Información y modificaciones a los existentes en el Ministerio que cuenten con el análisis e implementación de criterios de seguridad del software.
b. La Oficina de Tecnologías de la Información debe contar con mecanismos para justificar, acordar y documentar en la fase de requisitos y en la fase de modificación de los sistemas del Ministerio, los criterios de Seguridad de la Información.
c. La Oficina de Tecnologías de la Información debe contar en los requisitos de Seguridad de la Información los siguientes criterios:
    - El suministro de acceso y de autorización para usuarios del Ministerio, al igual que para usuarios privilegiados o técnicos.
    - Informar a los usuarios y operadores sobre sus deberes y responsabilidades.
    - Requisitos derivados de los procesos como registro de transacciones, seguimiento y no repudio.
d. La Oficina de Tecnologías de la Información debe definir controles para la transferencia de información a través de redes públicas para las aplicaciones del Ministerio.
e. La Oficina de Tecnologías de la Información debe disponer de controles para realizar transferencias completas, sin alteraciones y visualizaciones no autorizadas de la información entre las aplicaciones del Ministerio, teniendo en cuenta los siguientes criterios:
    - Contar con información de autenticación secreta de usuario.
    - Mantener privacidad en las partes involucradas.
    - Cifrar las comunicaciones cuando sea necesario.
    - Los protocolos de comunicación estén asegurados.
    - La información almacenada de las transacciones no se encuentre pública.

Código: SI-A.14.2 – Seguridad en los procesos de desarrollo y de soporte.
Propósito: Establecer lineamientos para que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información de la Entidad.
Lineamientos:

f. La Oficina de Tecnologías de la Información debe establecer los mecanismos necesarios para la creación de software, teniendo en cuenta los siguientes aspectos:
    - Orientar sobre buenas prácticas de seguridad en el desarrollo del software.

- Requisitos de seguridad en el control de versiones.
- Capacidad de los desarrolladores para evitar, encontrar y resolver vulnerabilidades.

g. La Oficina de Tecnologías de la Información debe tener en cuenta el punto anterior para la reutilización de códigos.

h. La Oficina de Tecnologías de la Información debe proteger los códigos ejecutables y código de desarrollo o compiladores del software operacional y aplicaciones propios del Ministerio.

i. La Oficina de Tecnologías de la Información debe definir controles para que los cambios de los Sistemas de Información en el Ministerio sean documentados, teniendo en cuenta la integridad de los sistemas desde las primeras etapas de diseño y a través de los mantenimientos posteriores.

j. La Oficina de Tecnologías de la Información debe definir un proceso formal para inclusión y cambios importantes de los Sistemas de Información involucrando pruebas, control de calidad e implementación.

k. La Oficina de Tecnologías de la Información debe definir para los cambios de los Sistemas del Ministerio los siguientes aspectos:
   - Niveles de autorización acordados.
   - Presentar los cambios a los usuarios autorizados.
   - Revisar la integridad para asegurar que no se vean comprometidos los cambios.
   - Identificar y validar el código crítico de seguridad.
   - Antes de cualquier cambio, asegurar que los usuarios autorizados aceptan los cambios.
   - Mantener un control de versiones para las actualizaciones de los sistemas.
   - Mantener un rastro de auditoria de los cambios.
   - Asegurar que los cambios se hagan en momentos adecuados y que no afecten los procesos del Ministerio.

l. La Oficina de Tecnologías de la Información debe guardar en un repositorio, las versiones anteriores de cada sistema de información que es actualizado.

m. La Oficina de Tecnologías de la Información debe definir la manera de revisar después de un cambio importante que el Sistema de Información alterado no se haya comprometido.

n. La Oficina de Tecnologías de la Información debe definir la manera para notificar a tiempo los cambios de los sistemas, permitiendo realizar pruebas y revisiones apropiadas antes de su implementación.

o. La Oficina de Tecnologías de la Información debe evitar las modificaciones a los paquetes de software, en la medida de lo posible se deberán usar directamente los dados por el proveedor; limitándose únicamente a cambios necesarios, cuando se hagan, se deberán tener en cuenta los siguientes aspectos:
   - El riesgo en que se puede ver involucrado el Sistema de Información.
   - Verificar si se requiere consentimiento del vendedor.
   - Verificar la posibilidad que el vendedor realice dichos cambios.

- El impacto en dado caso que el mantenimiento futuro recaiga en manos del Ministerio.
- La compatibilidad con otro software en uso.

p. La Oficina de Tecnologías de la Información debe conservar el software original cuando se hayan realizado cambios en los paquetes del mismo.

q. La Oficina de Tecnologías de la Información debe documentar el desarrollo de sistemas de información basado en los principios de seguridad l.

r. La Oficina de Tecnologías de la Información debe realizar verificación periódica a la documentación de los sistemas de información seguros en relación a los estándares de seguridad que hayan surgido y amenazas potenciales.

s. La Oficina de Tecnologías de la Información debe definir ambientes de desarrollo seguro, teniendo en cuenta los siguientes aspectos:

- El carácter sensible de los datos que el sistema va a procesar, almacenar y transmitir.
- Requisitos externos como reglamentaciones o políticas.
- Controles de Seguridad ya establecidos por el Ministerio.
- Separación entre diferentes ambientes de desarrollo.
- Control de acceso al ambiente de desarrollo.
- Seguimiento de los cambios en el ambiente y los códigos almacenados allí.
- Control sobre el movimiento de datos desde y hacia el ambiente.

t. La Oficina de Tecnologías de la Información debe definir controles para que los sistemas adquiridos externamente cumplan con los siguientes aspectos:

- Acuerdos de licenciamiento, propiedad de códigos y derechos de propiedad intelectual relacionados con el contenido contratado externamente.
- Requisitos contractuales para prácticas seguras de diseño, codificación y pruebas.
- Evidencia del uso de umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad.
- Evidencia de pruebas para vigilar que no exista contenido malicioso intencional y no intencional en el momento de la entrega.
- Evidencia de pruebas para proteger contra la presencia de vulnerabilidades conocidas.
- Derecho contractual con relación a procesos y controles de desarrollo de auditorías.
- Documentación del ambiente de construcción usado para crear entregables.

u. La Oficina de Tecnologías de la Información debe contemplar en los cambios y en los nuevos Sistemas de Información, pruebas asociadas a Seguridad de la Información.

v. La Oficina de Tecnologías de la Información debe contar en sus pruebas de aceptación de sistemas de información requisitos de Seguridad de la Información.

w. La Oficina de Tecnologías de la Información debe proporcionar repositorios de archivos fuente de los sistemas de información; estos deberán contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.
x. Los desarrolladores deberán asegurar la confiabilidad de los controles de autenticación, utilizando implementaciones centralizadas para dichos controles.
y. Los desarrolladores deberán establecer los controles de autenticación de tal manera que cuando fallen, lo hagan de una forma segura, evitando indicar específicamente cual fue la falla durante el proceso de autenticación y, en su lugar, generando mensajes generales de falla.
z. Los desarrolladores deberán asegurar que no se despliegan en la pantalla las contraseñas ingresadas, así como deberán deshabilitar la funcionalidad de recordar campos de contraseñas.
aa. Los desarrolladores deberán asegurar que se inhabilitan las cuentas luego de un número establecido de intentos fallidos de ingreso a los sistemas desarrollados.
bb. Los desarrolladores deberán asegurar que, si se utiliza la reasignación de contraseñas, únicamente se envíe un enlace o contraseñas temporales a cuentas de correo electrónico previamente registradas en los aplicativos, los cuales deberán tener un periodo de validez establecido; se deberán forzar el cambio de las contraseñas temporales después de su utilización.
cc. Los desarrolladores deberán establecer que periódicamente se valide la autorización de los usuarios en los aplicativos y se asegure que sus privilegios no han sido modificados.

Código: SI-A.14.3 – Datos de prueba.
Propósito: Establecer lineamientos para proteger los datos usados para pruebas.
Lineamientos:

dd. La Oficina de Tecnologías de la Información debe evitar durante la ejecución de pruebas en ambientes de desarrollo el uso de datos que contengan información personal o información sensible del Ministerio que este contenida en el ambiente de producción de las aplicaciones.
ee. La Oficina de Tecnologías de la Información debe tener en cuenta controles de acceso a los ambientes de producción y de prueba.

7.10. LINEAMIENTOS DE SEGURIDAD PARA LA RELACIÓN CON LOS PROVEEDORES

Código: SI-A.15.1 – Seguridad de la información en las relaciones con los proveedores.
Propósito: Establecer lineamientos para asegurar la protección de los activos de la organización que son accesibles a proveedores de la Entidad.
Lineamientos:

a. Grupo Interno de Trabajo de Contratación debe establecer lineamientos para el cumplimiento de las obligaciones contractuales de la dimensión de Seguridad y Privacidad de la Información con terceros o proveedores.
b. Grupo Interno de Trabajo de Contratación debe establecer en el momento de suscribirse contratos de cualquier tipo los riesgos asociados a la seguridad y privacidad de la información, los compromisos establecidos de confidencialidad de la información y el cumplimiento de las políticas de seguridad de la información del Ministerio.
c. Grupo Interno de Trabajo de Contratación deberá establecer en los contratos con terceros y proveedores los requisitos legales y regulatorios relacionados con la protección de datos personales, los derechos de propiedad intelectual y derechos de autor.
d. La Oficina de Tecnologías de la Información debe documentar, establecer controles y permisos cuando un tercero o proveedor requiera tener accesos a la información por medio de la infraestructura tecnológica del Ministerio.
e. La Oficina de Tecnologías de la Información debe verificar mensualmente el cumplimiento de Acuerdos de Nivel de Servicio establecidos con sus proveedores de tecnología.
f. La Oficina de Tecnologías de la Información debe establecer un procedimiento que permita asegurar la gestión de cambios a nivel de infraestructura, aplicativos y servicios tecnológicos que son soportados por terceros y/o proveedores, para garantizar estándares de eficiencia, seguridad, calidad y que permitan determinar los responsables y tareas a seguir para garantizar el éxito en la gestión de cambios.
g. Cada dependencia del Ministerio que establezca relación con proveedores y su cadena de suministro, debe solicitar acompañamiento periódico a la dimensión de Seguridad y Privacidad de la Información con el fin de dar a conocer las políticas que tiene el Ministerio.
h. El Grupo Interno de Trabajo de Contratación debe incluir en las guías de contratación y supervisión obligaciones generales sobre seguridad y privacidad de la información y los formatos para su cumplimiento y verificación por parte del supervisor de contrato.

7.11. LINEAMIENTOS PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Código: SI-A.16 – Gestión de incidentes de seguridad de la información y mejoras.
Propósito: Establecer lineamientos para asegurar una administración de incidentes de seguridad de la información coherente y eficaz con base a un enfoque de comunicación de los eventos y las debilidades de seguridad de la Entidad.
Lineamientos:

a. La Oficina de Tecnologías de la Información en conjunto con el Oficial de Seguridad de la Información y la Subdirección Administrativa y de Gestión Humana debe definir un procedimiento para la gestión de incidentes de seguridad de la información.
b. La Oficina de Tecnologías de la Información debe definir los canales para que los colaboradores del Ministerio puedan reportar los incidentes de Seguridad de la Información.
c. La Oficina de Tecnologías de la Información es la encargada de la evaluación de eventos de seguridad de la información y la decisión tomada sobre los mismos.
d. La Oficina de Tecnologías de la Información es la encargada para la recolección de evidencias de los incidentes de seguridad de la información.
e. La Oficina de Tecnologías de la Información debe contar con los mecanismos para el cumplimiento de los tiempos en la respuesta de incidentes establecido en los lineamientos para la Gestión de Incidentes.
f. La Oficina de Tecnologías de la Información debe proporcionar los medios para el aprendizaje al Ministerio de los incidentes de Seguridad de la Información.
g. La Oficina de Tecnologías de la Información deberá dar a conocer a los colaboradores del Ministerio los lineamientos establecidos para la Gestión de Incidentes de Seguridad de la Información.

7.12. LINEAMIENTOS PARA DEFINIR LOS ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE LA OPERACIÓN.

Código: SI-A.17.1 – Planificación de la Continuidad de la Seguridad de la Información.
Propósito: Establecer lineamientos para asegurar y mantener la seguridad de la información integrada en la gestión de continuidad de la operación de la Entidad.
Lineamientos:

a. La Oficina Asesora de Planeación y Estudios Sectoriales en conjunto con el Oficial de Seguridad de la Información y la Oficina de Tecnologías de la información deben diseñar una metodología para la identificación y evaluación de riesgos de continuidad de la operación de los servicios del Ministerio.
b. La Oficina Asesora de Planeación y Estudios Sectoriales en conjunto con el Oficial de Seguridad de la Información y la Oficina de Tecnologías de la información deben desarrollar

un análisis de impacto al negocio (BIA por sus siglas en ingles), por medio del cual se identifiquen los servicios críticos Ministerio.

c. La Oficina Asesora de Planeación y Estudios Sectoriales en conjunto con el Oficial de Seguridad de la Información y la Oficina de Tecnologías de la información, en coordinación con los lideres de procesos deben diseñar las estrategias y tiempos de recuperación de la operación de los servicios críticos del Ministerio.
d. La Oficina Asesora de Planeación y Estudios Sectoriales en conjunto con el Oficial de Seguridad de la Información y la Oficina de Tecnologías de la información deben realizar un plan de pruebas del plan de continuidad de la operación y deberá ser ejecutado mínimo 2 veces al año.
e. El plan de continuidad del negocio debe ser revisado en sesión de Comité MIG como minino una vez al año o cuando ocurra un cambio en el contexto interno o externos del Ministerio.
f. La Oficina de Tecnologías de la Información debe disponer de planes de contingencia de los servicios de TIC y un plan de recuperación ante desastres, enfocados a lograr el retorno a la operación normal.
g. El Grupo Interno de Contratación debe incluir en los procesos una obligación general que obligue a los contratistas a disponer de planes de contingencia y se deberá analizar su cobertura y alcance.
h. Se debe estructurar el Plan de Continuidad de la Operación acorde al alcance del sistema de gestión de Seguridad de la Información en coordinación con los líderes de los procesos, conforme a la normativa interna vigente.
i. El Plan de Continuidad de la Operación debe ser comunicado al interior del Ministerio
j. En caso de presentarse un incidente significativo que conlleve una interrupción se deberá gestionar el manejo de la crisis y los mecanismos de comunicación apropiados tanto internos como externos durante el estado de contingencia.
k. La Subdirección Administrativa y de Gestión Humana debe garantizar la integración de los planes de emergencia y contingencia con el plan de continuidad de la operación de los servicios del Ministerio.
l. El comité MIG debe definir un equipo para la planeación de pruebas, los procesos que estarán involucrados, la infraestructura tecnológica y/u operativa requerida, el plan de rollback y las actividades a realizar. Los participantes de los equipos deberán recibir sensibilización con respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre.
m. El equipo de pruebas del plan de continuidad debe documentar las pruebas y generar reportes o informes después de cada prueba y/o ejercicio que incluya recomendaciones, lecciones aprendidas y acciones para mejorar el plan y presentarlas al Comité MIG.
n. Se deben ejecutar procedimientos de control de cambios según las acciones preventivas y correctivas que se generaron a partir de las pruebas, para asegurar que el Plan de Continuidad se mantenga actualizado y mejorado.

o. El Oficial de Seguridad debe revisar y aprobar todas las estrategias de continuidad.

Código: SI-A.17.2 – Disponibilidad de instalaciones de procesamiento de información.
Propósito: Establecer lineamientos para asegurar la disponibilidad de las instalaciones de procesamiento de información de la Entidad.
Lineamientos:

a. La Oficina de Tecnologías de la información, la Subdirección Administrativa y la Oficina Asesora de Planeación y Estudios Sectoriales, deben implementar redundancia suficiente, para lo cual deberá considerar componentes o arquitecturas redundantes.
b. El equipo de pruebas del Plan de Continuidad debe poner a prueba los componentes o arquitecturas redundantes implementadas para asegurar que después de una falla el componente funcione.

7.13. LINEAMIENTOS PARA EL CUMPLIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN.

Código: SI-A.18.1 – Cumplimiento de los requisitos legales y contractuales.
Propósito: Establecer lineamientos para evitar incumplimientos a requisitos relacionados con la seguridad de la información de cualquier tipo especialmente a las obligaciones legales, estatutarias, normativas o contractuales.
Lineamientos:

a. La Oficina Asesora Jurídica debe definir y establecer un procedimiento y una herramienta que permita la revisión y de verificación del cumplimiento de los requisitos legales y reglamentarios en materia de Seguridad y Privacidad de la Información.
b. El Oficial de Seguridad de la Información en conjunto con la Oficina Asesora Jurídica deben identificar, documentar y actualizar todos los requerimientos contractuales, estatutarios y reglamentarios que puedan afectar los sistemas de Información del Ministerio, utilizando la herramienta de verificación de requisitos legales.
c. La Oficina de Tecnologías de la Información debe definir controles con el objetivo de proteger adecuadamente la propiedad intelectual del Ministerio, tales como derechos de autor de software, licencias y código fuente. El material registrado con derechos de autor no se debe copiar sin la autorización del propietario.
d. La Oficina Asesora de Prensa debe generar campañas de comunicación con el fin de apropiar a los colaboradores Ministerio sobre el uso de los derechos de propiedad intelectual (no copiar total ni parcialmente libros, artículo u otros documentos diferentes de los permitidos por la ley de derechos de autor.)
e. La Subdirección Administrativa y de Gestión Humana debe generar directrices sobre retención, almacenamiento, manipulación y eliminación de registros e información física y digital del Ministerio.

f. La Subdirección Administrativa y de Gestión Humana debe establecer e implementar controles para proteger los registros contra pérdida, destrucción y falsificación de información física y digital.
g. La Subdirección Administrativa y de Gestión Humana debe establecer procedimientos de almacenamiento a largo plazo y manipulación de los registros físicos y digitales.
h. El Oficial de Seguridad de la Información, la Oficina Asesora Jurídica, deben definir o actualizar cuando sea necesario la política de tratamiento de datos personales, para la protección de los derechos fundamentales de la información de los ciudadanos en su tratamiento.
i. El Grupo Interno de Trabajo de Contratación debe incluir los mecanismos para que los supervisores de contrato validen el cumplimiento de las obligaciones generales en materia de seguridad y privacidad de la información.

Código: SI-A.18.2 – Revisiones de la seguridad de la información.
Propósito: Establecer lineamientos para garantizar que se implementa y opera la seguridad de la información de acuerdo a las políticas y procedimientos organizacionales
Lineamientos:

a. La Oficina de Control Interno, deberá realizar de manera periódica auditorías internas para comprobar el correcto funcionamiento del Sistema de Gestión de Seguridad de la Información en cuanto a los objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información.
b. Los líderes de los procesos deberán asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad se realicen correctamente, con el fin de cumplir las políticas y normas de seguridad; en caso de incumplimiento se evaluarán y propondrán acciones correctivas. Los resultados de estas revisiones serán mantenidos para su revisión en auditorías.
c. La Oficina de Tecnologías de la Información debe comprobar periódicamente que los sistemas de información cumplen con las normas de implementación de seguridad. Se deberán realizar auditorías periódicas con ayuda de herramientas automatizadas y se deberán generar informes técnicos.

Control de Cambios		
Fecha	**Versión**	**Descripción**
26/03/2019	1.0	Creación del documento.

Elaboró: Andrés Díaz Molina – Asesor Despacho de la Ministra encargado de las funciones de Oficial de Seguridad de la Información
Erika T. Quintero – Contratista Seguridad de la Información – Oficina de Tecnologías de la Información

Revisó y Aprobó: Comité MIG, Sesión del 26 de marzo de 2019