MINISTERIO DE VIVIENDA, CIUDAD Y TERRITORIO

MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

2023

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Las exigencias de seguridad requeridas actualmente frente al esquema de globalización de lastecnologías de información y comunicaciones (TIC), hace necesario que las instituciones de índole privada y pública, desarrollen políticas que contrarresten la aparición de nuevas amenazas en los sistemas computarizados, tales como las transgresiones e intrusiones cibernéticas, que atentan contrala estabilidad y el normal funcionamiento de los servicios que presta la Oficina de Tecnologías de la Información y las Comunicaciones. De igual forma y para asegurar la información desde todos los ángulos, es importante desarrollar conciencia en todos los servidores públicos de la responsabilidad que tienen frente a los activos de información que cada uno tiene a cargo.

El Ministerio de Vivienda, Ciudad y Territorio como líder del sector (Vivienda, Ciudad y Territorio) para garantizar su competencia tiene la responsabilidad de contar con un direccionamiento estratégico en materia de seguridad de los activos de información propios de su ambiente institucional.

El presente manual hace parte integral de la resolución No. 0973 del 28 de diciembre de 2017 "*Por la cual se adopta el Sistema de Gestión de Seguridad de la Información SGSI, la Política y los Objetivos de Seguridad de la Información en el Ministerio de Vivienda, Ciudad y Territorio, en el marco de la estrategia de Gobierno en Línea*", o de la que la modifique o derogue.

El Decreto 1078 de 2015 dispone que las entidades que conforman la administración pública serán sujetos obligados para el cumplimiento de las políticas y los lineamientos de la Estrategia de Gobierno en Línea, estableciendo en su artículo 2.2.9.1.2.1 como uno de sus componentes el de la Seguridad y Privacidad de la Información, comprendido por las acciones transversales a los componentes de TIC para Servicios, TIC para el Gobierno Abierto y TIC para la Gestión, tendientes a proteger la información y sistemas de información, del acceso, divulgación, interrupción o destrucción no autorizada, que mediante el Decreto 1008 de 2018 se definieron los lineamientos para evolucionar de la "*Estrategia de Gobierno en Línea*" a la "*Política de Gobierno Digital*". Que el artículo 2.2.9.1.2.1. Estructura. En el numeral 2 enuncia "*Habilitadores Transversales de la Política de Gobierno Digital: Son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital*", entre otra normatividad del Gobierno Nacional.

Las políticas generales y específicas de seguridad y privacidad de la

información se fundamentan en los dominios y objetivos de control de la norma ISO/IEC 27001:2013 y en el código de buenas prácticaspara la gestión de la seguridad de la información ISO/IEC 27002:2013 y en el Modelo de Seguridad y Privacidad de la Información MSPI.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Definir los lineamientos, políticas generales y específicas que deben cumplir todos los funcionarios,contratistas y terceros del Ministerio de Vivienda, Ciudad y Territorio, frente a amenazas internaso externas, deliberadas o accidentales, para garantizar y preservar la confidencialidad, integridad y disponibilidad de los activos de la información.

2.2 OBJETIVO ESPECÍFICOS

i. Definir los roles y responsabilidades para la implementación, seguimiento y mejora del SGSI,
ii. Sensibilizar sobre los requerimientos técnicos del estándar ISO/IEC 27001:2013 de Seguridad de la Información, la cual establece los requerimientos para el establecimiento, implementación y mejoramiento continuo del sistema de gestión de seguridad de la información y del Modelo de Seguridad y Privacidad de la Información MSPI del Gobierno Nacional necesarios para la implementación, seguimiento y mejora del sistema de gestión de seguridad de la información.
iii. Orientar la implementación del SGSI al interior del Ministerio de Vivienda, Ciudad y Territorio.

3. ALCANCE

Este documento aplica a todos los niveles y sedes del Ministerio, funcionarios, directivos, terceros tales como proveedores y contratistas, entes de control, usuarios internos y externos que accedan o hacen uso de cualquier activo de información, independientemente de su ubicación, medio o formato.

Las políticas aplican a toda la información creada, procesada y/o utilizada en el soporte y desarrollo de las funciones y competencias del MVCT, sin importar el medio, formato, presentación o lugar en el cual se encuentre. Toda

información debe contar con mecanismos y disposiciones que garanticen su confidencialidad, integridad, disponibilidad y autenticidad.

4. COMPROMISO DE LA ALTA DIRECCIÓN

El Ministro de Vivienda, Ciudad y Territorio se encargará de liderar y asegurar la sostenibilidad y mejoramiento continuo del Sistema de Gestión de Seguridad de la información - SGSI de conformidad con el alcance establecido.

5. COMPETENCIA

La sostenibilidad y mejoramiento del sistema de gestión de seguridad de la información – SGSI, estará a cargo de colaboradores de la Oficina de Tecnologías de la Información y las Comunicaciones (TIC), quienes deberán acreditar la educación, formación y experiencia requerida por el Ministerio, de acuerdo con el rol que desempeñen.

Las competencias en formación y experiencia del o los colaboradores para la implementación y sostenimiento del SGSI, son:

Profesionales en Ingeniería de sistemas, Ingeniero de sistemas con énfasis en telecomunicaciones, Ingeniero Telemático o Ingeniero Electrónico.

Preferiblemente certificados en auditoria en la norma NTC-ISO 27001:2013, con las normas concordantes y vigentes.

En cuanto a experiencia se requiere mínimo 12 meses de experiencia profesional relacionada.

Las competencias en formación y experiencia del oficial de seguridad de la información están descritas en el numeral 7.3.2 de este manual.

6. ¿QUÉ ES SEGURIDAD DE LA INFORMACIÓN?

La información es un activo que, como otros activos importantes, es esencial y en consecuencia necesita ser protegido. La información puede existir en muchas formas, puede estar impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, mostrada en videos o hablada en una conversación. Cualquiera que sea la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre deberá estar apropiadamente protegida.

La seguridad de la información es la protección de esta en un rango amplio de

amenazas y vulnerabilidades, que busca que toda entidad no interrumpa los servicios esenciales para la cual fue creada. La seguridad de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procedimientos, estructuras organizacionales y funciones de software y hardware, entre otras. Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad, funcionalidad y operación específicos. Esto debe ser realizado en conjunto con todos los demás procesos del Ministerio.

7. ROLES Y RESPONSABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN

Resulta importante al interior del Ministerio generar una cultura organizacional a partir de la puesta en marcha de roles y responsabilidades para la adecuada gestión de la seguridad de la información. Para que esto sea posible, se requiere la coordinación de esfuerzos entre los funcionarios y/o contratistas de las diferentes dependencias del Ministerio en función de propiciar medidas de protección sobre los datos e información de la entidad.

Los roles y responsabilidades del SGSI para el MVCT deben interactuar de manera articulada para la implementación, seguimiento y mejora del sistema de gestión, basado en el Modelo de Seguridad y Privacidad de la Información MSPI, estos roles son:

- Instancia orientadora del SGSI.
- Líder para la implementación, seguimiento y mejora del SGSI.
- Oficial de Seguridad de la Información.
- Servidores públicos del MVCT.
- Equipo técnico de seguridad de la información
- Líderes de los procesos
- Colaboradores del MVCT.
- Grupos de interés.

7.1 INSTANCIA ORIENTADORA DEL SGSI

Es la máxima instancia del SGSI y es responsable de emitir las políticas y tomar decisiones estratégicas para la implementación, seguimiento y mejoramiento continuo del sistema. Este rol lo desempeña el Comité Institucional de Gestión y Desempeño del Ministerio de Vivienda, Ciudad y Territorio, de acuerdo con lo estipulado en el artículo tercero de la resolución 0958 del 24 de diciembre de 2019, del cual se desprenden las responsabilidades que se refieren a

continuación.

Todos los integrantes del Comité Institucional de Gestión y Desempeño apoyarán con su liderazgo y promoverán el compromiso en las personas que hacen parte de los equipos que tengan a cargo, con la sostenibilidad y mejora continua del SGSI.

7.1.1 Responsabilidades de la instancia orientadora del SGSI

1. Aprobar las políticas de gestión y directrices en materia de gobierno digital, seguridad digital y de la información.
2. Coordinar la implementación, sostenibilidad, seguimiento y mejora continua del SGSI al interior del MVCT.
3. Aprobar los recursos que se requieran para la sostenibilidad y mejoramiento continuo del SGSI.
4. Mantener informado al señor Ministro sobre el desempeño del SGSI.
5. Acompañar e impulsar el desarrollo de proyectos de seguridad que presente el líder del sistema en aras del mejoramiento de este.
6. Aprobar los roles y responsabilidades específicos que se relacionen con la seguridad de la información.
7. Aprobar el plan de acción del SGSI.
8. Apoyar las acciones que permitan apropiar los recursos necesarios para abordar los riesgos, las oportunidades de mejora y demás hallazgos, en pro de brindar servicios con calidad y seguridad.
9. Realizar revisiones periódicas del SGSI, de por lo menos una vez al año, con el fin de asegurar la conveniencia, adecuación, eficacia, eficiencia, efectividad y alineación continúa con el marco estratégico de la entidad.
10. Las demás funciones inherentes a la naturaleza del Comité.

7.2 LÍDER PARA LA IMPLEMENTACIÓN, SEGUIMIENTO Y MEJORA DEL SGSI

El Líder del SGSI, es el Jefe de la Oficina de Tecnología de la Información y las Comunicaciones - TIC, quien se encargará de planear, disponer y utilizar los recursos de su competencia para la implementación, sostenibilidad y mejoramiento continuo del Sistema.

7.2.1 Responsabilidades del líder del SGSI

1. Proponer políticas, objetivos y planes en el marco del SGSI e implementar estrategias para la sostenibilidad y mejora continua del mismo, en coordinación con la Oficina Asesora de Planeación.
2. Revisar y presentar el plan de acción del SGSI ante la instancia orientadora

del SGSI.

3. Presentar ante la instancia orientadora del SGSI, informes y/o propuestas sobre la gestión y desempeño del SGSI.
4. Gestionar los recursos necesarios para la implementación, sostenibilidad y mejora del SGSI.
5. Asesorar técnicamente a otros procesos en temas relacionados con el SGSI.
6. Determinar la necesidad de cambios del SGSI.
7. Liderar la gestión de riesgos de seguridad de la información y seguridad digital en coordinación con la Oficina Asesora de Planeación.
8. Gestionar la elaboración de piezas de comunicación relacionadas con la difusión, sostenibilidad y mejoramiento continuo del SGSI, bajo los lineamientos institucionales de imagen corporativa, en coordinación con la Oficina Asesora de Planeación y el Grupo de Comunicaciones Estratégicas.
9. Realizar las acciones y gestiones necesarias para el cumplimiento de la política y los objetivos
10. Presentar para aprobación de la instancia orientadora los ajustes y actualizaciones de la política de seguridad de la información y del manual de políticas de seguridad y privacidad de la información y seguridad digital, cuando se requiera.
11. Realizar seguimiento a la gestión de incidentes de seguridad de la información.
12. Reportar, ante la instancia orientadora del sistema, los incidentes catalogados como catastróficos.
13. Aprobar los indicadores del SGSI.
14. Aprobar los informes y reportes relacionados con el SGSI, que soliciten los entes de control y demás partes interesadas internas y externas del Ministerio.
15. Promover que los requisitos legales y requisitos de las partes interesadas del SGSI, se identifiquen y cumplan de acuerdo con las normas vigentes y el procedimiento definido en el Ministerio.
16. Coordinar, retroalimentar y representar al equipo técnico responsable de implementar el SGSI ante las diferentes instancias, y revisar anualmente su conformación.
17. Monitorear y realizar seguimiento a la implementación del SGSI.
18. Las demás que conforme a las disposiciones legales deba desarrollar.

7.3 OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

El oficial de seguridad de la información lidera la implementación de las políticas, lineamientos, directrices y planes, que definan la instancia orientadora y/o el líder del sistema.

El oficial de seguridad de la información en la Entidad será el funcionario designado por el Ministro de Vivienda, Ciudad y Territorio para tal fin a través de resolución.

7.3.1 Responsabilidades del oficial de seguridad de la información

1. Proponer y apoyar en la definición de políticas y objetivos del SGSI.
2. Presentar propuestas e implementar estrategias para la sostenibilidad y mejora del sistema.
3. Formular y monitorear los indicadores del SGSI.
4. Apoyar a los procesos en la identificación y actualización de los activos de información.
5. Acompañar a los diferentes procesos en la identificación, evaluación y planeación de las acciones requeridas para mitigar los riesgos propendiendo por la sostenibilidad y mejora de la seguridad de la información.
6. Asesorar técnicamente a otros procesos en temas relacionados con seguridad de la información.
7. Elaborar el plan de acción del SGSI.
8. Proponer cambios al SGSI.
9. Realizar campañas de concienciación en temas referentes a seguridad de la información al interior del Ministerio.
10. Realizar las acciones y gestiones necesarias para el cumplimiento de la política y los objetivos del SGSI, lo cual incluye brindar o gestionar ante las dependencias que corresponda las acciones a que haya lugar.
11. Participar en los espacios de capacitación establecidos por el Ministerio en el plan de implementación y capacitación para el fortalecimiento del SGSI, incluidos en el plan de uso y apropiación de TI.
12. Actualizar la documentación del SGSI.
13. Establecer y apoyar en la implementación de los controles tecnológicos de seguridad de la información en el Ministerio.
14. Consolidar la matriz de activos de seguridad de la información.
15. Comunicar los incidentes de seguridad de la información al Líder del sistema.
16. Emitir orientaciones que propendan que la información del MVCT se encuentre protegida apropiadamente, sobre los pilares de la confidencialidad, la integridad y la disponibilidad de la información, así como de los recursos informáticos y físicos que la soportan.
17. Alinear el sistema de gestión de seguridad de la información- SGSI del Ministerio, con la estrategia del modelo de privacidad y seguridad de la información, así como la ciberdefensa y ciberseguridad del Estado Colombiano y los lineamientos del Gobierno Nacional disponga para la

seguridad de la información.
18. Las demás asignadas por el Líder del sistema de gestión de seguridad de la información.

7.3.2 Competencia en información y experiencia del oficial de seguridad de la información

El oficial de seguridad de la información para el Ministerio deberá contar con la siguiente formación y experiencia mínima:

Profesional en Ingeniería de sistemas, Ingeniero de sistemas con énfasis en telecomunicaciones, Ingeniero Telemático o Ingeniero Electrónico.

En cuanto a experiencia se requiere mínimo 28 meses de experiencia profesional relacionada.

7.4 SERVIDORES PÚBLICOS DEL MVCT

7.4.1 Equipo técnico de seguridad de la información

El Equipo Técnico de Seguridad de la Información SGSI, es una instancia consultiva conformada por representantes de algunos procesos, el cual será convocado por él Oficial de Seguridad de la Información y está conformado por:

- Proceso de Gestión de las Tecnologías de la Información y las Comunicaciones, Cargo: Jefe Oficina de Tecnologías de Información y las Comunicaciones.
- Proceso: Direccionamiento Estratégico, Cargo: Jefe Oficina Asesora de Planeación.
- Proceso: Seguimiento y Mejora continua, Cargo: Jefe Oficina Asesora de Planeación.
- Proceso: Gestión de Recursos Físicos, Cargo: Subdirector de Servicios Administrativos.
- Proceso: Gestión Documental, Cargo: Subdirector de Servicios Administrativos.
- Proceso: Gestión Estratégica del Talento Humano, Cargo: Coordinador Grupo de Talento Humano.
- Proceso: Gestión de Contratación, Cargo: Subdirector de Servicios Administrativos.
- Proceso: Conceptos Jurídicos, Cargo: Jefe Oficina Asesora Jurídica, y el

- Proceso: Evaluación, Independiente y Asesoría, Cargo: Jefe Oficina de Control Interno, será invitado permanente a las reuniones del equipo técnico de seguridad de la información, y participará con voz, pero sin derecho a voto.

7.4.1.1 Responsabilidades del equipo técnico

1. Conceptuar sobre el plan de acción del SGSI.
2. Cumplir los compromisos o actividades que queden bajo su responsabilidad en el plan de acción del SGSI, en que participa y reportar las evidencias de su cumplimiento al Líder delsistema.
3. Apoyar al Líder del SGSI en la implementación del mismo en el Ministerio.
4. Asistir a las mesas de trabajo que sea requerido en temas de seguridad de la información.

Las convocatorias se realizan en el marco de las reuniones del Comité Institucional de Gestión yDesempeño de la Entidad.

7.4.2 Líderes de los procesos

Se denomina Líder de proceso (de acuerdo con las caracterizaciones definidas en el mapa de procesos) al cargo, responsable de la correcta ejecución de los procesos a su cargo y en general de la sostenibilidad y mejoramiento continuo del Sistema.

7.4.2.1 Responsabilidades de los líderes de los procesos

1. Gestionar (elaborar, modificar, eliminar, socializar e implementar) la documentación de su proceso.
2. Actualizar y aprobar la relación de los activos de información de su proceso.
3. Participar en las acciones de promoción y comunicación del sistema.
4. Identificar y tratar los riesgos de seguridad de la información y seguridad digital que pueden afectar los activos de información de los procesos.
5. Velar por el cumplimiento de las políticas y directrices definidas en el marco de la implementación del Sistema de Gestión de Seguridad de la Información, al interior de cada una de las dependencias que conforman los procesos del Sistema Integrado de Gestión del MVCT.
6. Las demás que conforme a las disposiciones legales puedan desarrollar.

7.4.3 Colaboradores MVCT

Este rol lo conforman todos los colaboradores (funcionarios y contratistas) que

hacen parte del Ministerio de Vivienda, Ciudad y Territorio.

7.4.3.1 Responsabilidades de los colaboradores del MVCT

1. Participar en las actividades de concienciación que se realicen en el marco del SGSI.
2. Reportar los incidentes de seguridad de la información.
3. Cumplir y acatar las políticas y lineamientos que se dicten en materia de seguridad de la información.
4. Participar en la identificación de los activos de información.
5. Participar en la identificación de los riesgos de seguridad de la información y seguridad digital, y participar en la gestión de los mismos.

7.5 RUPOS DE INTERES

Los grupos de interés están definidos en el numeral 11 como partes interesadas del presente manual (colaboradores, proveedores y/o terceras partes, usuarios y sociedad/comunidad), quienes deberán cumplir las políticas y lineamientos definidos en materia de seguridad de la información por el Ministerio de Vivienda, Ciudad y Territorio.

8. COMUNICACION

El Sistema de Gestión de Seguridad de la Información debe comunicarse a las partes internas y externas, para ello se tienen establecidas actividades de comunicación a través de los planes de Seguridad y Privacidad de la Información y del Plan de Sensibilización de Seguridad y Privacidad de la Información. A continuación, se listan los productos que deben comunicarse:

¿Qué comunica?	¿Quién lo comunica?	¿A quién lo comunica?	¿Cuándo lo comunica?	¿Cómo lo comunica?
Inventario de activos de formación SGSI	Oficial de Seguridad de la Información	Líderes de los procesos	Anual	Intranet
Listado de activos según Ley 1712 de	Oficial de Seguridad de la	Profesional que lidera la política de transparencia	Anual	Página web

2014	Información	de la Entidad		
Normograma	Oficial de Seguridad de la Información	Servidores públicos del MVCT	Cuando se requiera	Página web e Intranet
Matriz de riesgos de seguridad de la información SGSI	Oficial de Seguridad de la Información	Líderes de los procesos	Anual	Intranet
Boletines de Seguridad de la información	Oficial de Seguridad de la Información	Servidores públicos del MVCT	Cuando se requiera	Llavearías, correo electrónico y comunicaciones escritas
Reportes de incidentes relevantes.	Oficial de Seguridad de la Información	Líder para la implementación, seguimiento y mejora del SGSI	Cuando se requiera	Correo electrónico y comunicaciones escritas

9. DEFINICIONES Y ABREVIATURAS

NTC-ISO/IEC 27001:2013: Norma técnica colombiana que ha sido elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI).

- **Cliente:** Organización, entidad o persona que recibe un producto y/o servicio.
- **Eficacia:** Grado en el que se realizan las actividades planificadas y se alcanzan los resultados planificados.
- **Eficiencia:** Relación entre el resultado alcanzado y los recursos utilizados.
- **Efectividad:** Medida del impacto de la gestión tanto en el logro de los resultados planificados, como en el manejo de los recursos utilizados y disponibles.
- **Mejora continua:** Acción permanente realizada, con el fin de aumentar la capacidad para cumplir los requisitos y optimizar el desempeño.
- **Proceso:** Conjunto de actividades relacionadas mutuamente o que interactúan para generar valor y las cuales transforman elementos de entrada en resultados.
- **Producto o servicio:** Resultado de un proceso o un conjunto de procesos.
- **Trazabilidad:** Capacidad para seguir la historia, la aplicación o la

localización de todo aquello queestá bajo consideración.

- **Aceptación del riesgo**: decisión de asumir un riesgo.
- **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 misionales de MVCT.
- **Acuerdos de aceptación de las políticas de seguridad:** son documentos en los que los funcionarios del MVCT o provistos por terceras partes, aceptan acatar las políticas de seguridad de la información y se acogen a las sanciones establecidas por el incumplimiento de dichas políticas.
- **Acuerdos de confidencialidad:** son documentos en los que los funcionarios del MVCT o provistos por terceras partes, manifiestan su voluntad de mantener la confidencialidad de la información del Ministerio, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro del Ministerio.
- **Acuerdos de intercambio:** son documentos constituidos entre el MVCT y sus proveedores de servicios en donde se especifican las condiciones del intercambio de información, los compromisos de los proveedores de mantener la confidencialidad y la integridad de la información a la que tengan acceso en virtud de la labor que desarrollan para el Ministerio, las vigencias y las limitaciones a dichosacuerdos.
- **Acuerdos de niveles de servicio:** herramientas que ayudan a proveedores y clientes de un servicio determinado a llegar a un consenso en términos del nivel de calidad que se ha de alcanzar en el servicio contratado. Registran el entendimiento común de servicios, responsabilidades, garantías, tiempos de respuesta, horarios de disponibilidad, entre otros.
- **Administración de riesgos**: Proceso sistemático 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 enforma periódica
- **Amenaza:** causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización, la amenaza es una condición del entorno del sistema de información que, dada una oportunidad, podría dar lugar a que se ocasione una violación de la seguridad.
- **Áreas Seguras:** Son aquellas en donde se encuentren sistemas de procesamiento y almacenamiento informático o de datos.

  En el MVCT se identifican las siguientes áreas seguras:
  - Cuartos de cableado.
  - Centro de datos.

  - Archivos generales y de gestión.
  - Lugares que contengan información Reservada.
  - Áreas de pagaduría, entre otras.
- **Autenticidad:** busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- **Autenticación:** es el procedimiento de comprobación de la identidad de un usuario al tratar de acceder un recurso de procesamiento o sistema de información.
- **Autenticación Fuerte:** Se habla de autenticación fuerte cuando un sistema de autenticación utiliza por lo menos dos de los tres factores básicos de autenticación: algo que la persona sabe (contraseña, PIN, número de un documento personal, nombre de algún pariente, etc.) algo que la persona posee (credencial, tarjeta magnética, token, etc.) o algo que la persona es (reconocimiento facial, voz, iris, retina, etc.). De este modo, si uno de los factores se ve comprometido, todavía existe un segundo factor que garantiza la seguridad.
- **Cadena de Custodia:** es la aplicación de una serie de normas y/o procedimientos tendientes a asegurar, depositar y proteger cada activo de información para evitar la pérdida de integridad, disponibilidad o confidencialidad.
- **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**: Se identifica como foco de la ciberseguridad los activos digitales como datos, dispositivos y sistemas que permiten a la organización cumplir con sus objetivos de negocio.
- **Ciberactivo crítico**: Ciberactivo que es crítico para la operación de un activo crítico.
- **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 Institucional de Gestión y Desempeño:** es un cuerpo integrado por representantes de la alta dirección y el líder de seguridad de la información, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.
- **Confidencialidad:** propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados, la información es accesible solamente por quienes están autorizados para ello.
- **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.

- **Control:** medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, acciones, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal. NOTA. Control es también utilizado como sinónimo de salvaguarda.
- **CCOCI**: Comando Conjunto Cibernético, Unidad Militar Conjunta (Ejército, Armada y Fuerza Aérea),que tiene como función principal prevenir, detectar, orientar, contener, decidir, responder y recuperarante amenazas cibernéticas que afecten la sociedad, la soberanía nacional, independencia, integridad territorial, el orden constitucional y los intereses nacionales, todo esto, soportado en un marco jurídico y/o la Constitución Nacional.
- **COLCERT**: Por las siglas en inglés de Computer Emergency Response Team, es el Grupo de Respuesta a Emergencias Cibernéticas de Colombia, y tiene como responsabilidad central la coordinación de la Ciberseguridad y Ciberdefensa Nacional, la cual estará enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su propósito principal será la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de Ciberseguridad que atenten ocomprometan la seguridad y defensa nacional.
- **CSIRT**: Por las siglas en inglés de Computer Security Incident Response Team, es el equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional CSIRT-PONAL, creado para atender las necesidades de prevención, atención e investigación de los eventos e incidentes de seguridad informática, con el fin de proteger la infraestructura tecnológica, los activos de información y mitigar el impacto ocasionado por la materialización de los riesgos asociados con el uso de las tecnologías de la información y las telecomunicaciones.
- **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.
- **Derechos de Autor:** es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.
- **Disponibilidad**: propiedad de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.
- **Dispositivos móviles**: equipo de cómputo pequeño, cuyo concepto principal es la movilidad, el cualpermite almacenamiento limitado, acceso a internet y cuenta con capacidad de procesamiento.
- **Evaluación del riesgo:** evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma,

probabilidad de que ocurran y su potencial impacto.

- **Evento de seguridad de la información:** presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.
- **Gestión del riesgo:** actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.
  NOTA. La gestión de riesgos usualmente incluye la evaluación de riesgos, el tratamiento de riesgos, la aceptación de riesgos y la comunicación de riesgos.
- **Hacking ético:** es el conjunto de actividades para ingresar a las redes de datos y voz de una entidad con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo al cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.
- **Incidente de seguridad de la información:** un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer la confidencialidad, integridad y/o disponibilidad de la información y amenazar la seguridad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.
- **Información:** 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.
- **Infraestructura Crítica (IC)**: Son las infraestructuras estratégicas cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales. Adaptación Ley 8/2011-Gobierno de España.
- **Infraestructura Crítica Cibernética (ICC)**: Son las infraestructuras estratégicas soportadas por Tecnologías de Información y Comunicaciones (TIC) o Tecnologías de Operación (TO), cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales. Fuente: Ministerio de Defensa.
- **Integridad:** propiedad de salvaguardar la exactitud de la información y sus métodos de proceso y el estado completo de los activos.
- **Legalidad**: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la entidad
- **Líder de Seguridad de la Información:** Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los funcionarios del Ministerio que así lo requieran.

- **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 Servicio**: 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 Dirección de Información y Tecnología se informa de las necesidades que tienen los funcionarios en cuanto a los recursos informáticos a nivel nacional.
- **MVCT:** Ministerio de Vivienda, Ciudad y Territorio
- **No repudio:** se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- **Perfiles de usuario:** son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos informáticos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.
- **Plan de contingencia:** es un documento que describe en forma clara, concisa y concreta los riesgos, los actores, las responsabilidades y los procedimientos a seguir tendientes a restablecer la operación normal, en casos de eventos adversos. El Plan de Contingencia deberá inventariar los distintos procesos de negocio y determinar la dependencia e importancia que supone para el Ministerio en términos de disponibilidad. Para los procesos críticos se deberá destinar la máxima atención y recursos.
- **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 recuperación ante desastres:** hace parte del Plan de Contingencia y es un conjunto de procedimientos de recuperación de la plataforma tecnológica del Ministerio y cubre aspectos como los datos, el hardware y el software crítico, para que el Ministerio pueda restablecer sus operaciones en caso de un desastre natural o causado por humanos en forma rápida, eficiente y con el menor costo y pérdidas posibles. El Plan también debe incluir las consideraciones necesarias para enfrentarse a la pérdida inesperada o repentina de personal crítico.
- **Propiedad intelectual:** es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluidas las invenciones científicas y tecnológicas, las producciones literarias o artísticas,

las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

- **Propietarios de la Información:** Son los funcionarios o dependencias responsables de la generación o recopilación de la información, con competencia para administrar y disponer de su contenido.
- **Reasignación de derechos de acceso:** es la modificación de los privilegios con que cuenta un funcionario sobre un recurso informático, la red de datos del Ministerio o un sistema de información cuando cambia de funciones dentro del Ministerio.
- **Remoción de derechos de acceso:** es el bloqueo o la eliminación de los privilegios o de la cuenta de usuario de la cual dispone un funcionario sobre un recurso informático, la red de datos del Ministerio o un sistema de información.
- **Reducción del Riesgo:** Acciones que se toman para disminuir la probabilidad y/o las consecuencias negativas, o ambas, asociadas con un riesgo.
- **Riesgo:** combinación de la probabilidad de ocurrencia de un evento y sus consecuencias o impacto.
- **Riesgo residual:** nivel restante de riesgo después del tratamiento del riesgo.
- **Seguridad de la información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.
- **Sistema de gestión de la seguridad de la información – SGSI - :** Parte del sistema de gestión global, basado en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información (ciclo PHVA).
- **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 MVCT.
- **Software malicioso:** es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse en un computador o una red para dañar recursos informáticos, sistemas operativos, redes de datos o sistemas de información.
- **Soporte Técnico:** es un servicio que proporciona un único punto de contacto para todos los usuarios de servicios relacionados con tecnologías de información del Ministerio, respondiendo y dando solución a las preguntas y problemas. De igual manera, brinda un apoyo inmediato en línea acerca de los problemas relacionados con el software y hardware de las estaciones de trabajo y equipos portátiles. El Soporte Técnico resuelve requerimientos e

indica los pasos a seguir para solicitar los servicios proporcionados por el Grupo de Soporte Técnico y orienta dichas solicitudes al personal apropiado.
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.

- **Tratamiento del riesgo:** procesos de selección e implementación de medidas para modificar el riesgo.
- **Tecnología de la Información:** Conjunto de hardware y software operados por la entidad o por un tercero en su nombre, que componen la plataforma necesaria para procesar y administrar la información que requiere la entidad para llevar a cabo sus funciones.
- **Test de penetración**: es un ataque dirigido y controlado hacia componentes de infraestructura tecnológica para revelar malas configuraciones y vulnerabilidades explotables
- **Valoración del riesgo:** proceso global de análisis y evaluación del riesgo.
- **Vulnerabilidad:** debilidad de un activo o grupo de activos que puede ser aprovechada por una o másamenazas.
- **VPN:** Una red privada virtual de las siglas en inglés de Virtual Private Network, es una tecnología dered que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet.

10. PARTES INTERESADAS

Las partes interesadas corresponden a las personas naturales o jurídicas con la cuales el MVCT interactúa en el ejercicio de sus funciones, que pueden afectar o ser afectadas por la seguridad de la información del Ministerio y en algunos casos, pueden manifestar un interés directo, explícito y comprometido con los objetivos y propósitos del sistema de gestión de seguridad de la información - SGSI.

Las siguientes son las partes interesadas (internas y externas) del MVCT en función a la seguridad dela información:

Parte interesada	Necesidades	Expectativas	Requisitos en el sistema de gestión	Logros y resultados esperados

Colaboradores	Socializar y apropiar políticas, procedimientos y documentación del SGSI.	Cumplimiento de las políticas de Seguridad de la Información reduciendo las probabilidades de afectación a la información del MVCT.	Manual Políticas de Seguridad de la Información	Reducción de probabilidad de afectación a la información de los colaboradores del MVCT.
Proveedores y/o terceras partes	Socializar políticas, procedimientos y documentación del SGSI.	Cumplimiento de las políticas de Seguridad de la Información reduciendo las probabilidades de afectación a la información del MVCT	Manual Políticas de Seguridad de la Información.	Reducción de probabilidad de afectación a la información que custodie.
Usuarios	Protección de la información suministrada al MVCT.	Cumplimiento de las políticas de Seguridad de la Información reduciendo las probabilidades de afectación a la información del MVCT	Manual Políticas de Seguridad de la Información	Reducción de probabilidad de afectación a la información de los usuarios del MVCT
Sociedad / Comunidad	Propender por el adecuado tratamiento de los datos personales suministrados por los usuarios que acceden a los servicios del MVCT, de acuerdo con lo establecido en la Ley 1581 de 2012 y los procedimientos establecidos por la entidad.	Cumplir las políticas de Seguridad y privacidad de la Información, con el propósito de preservar la información custodiada por el MVCT	Manual Políticas de Seguridad de la Información	Reducción de probabilidad de afectación a la información de la sociedad y de la comunidad.

	Proteger, preservar y administrar la integridad,			

Gobierno

Parte interesada	Necesidades	Expectativas	Requisitos en el sistema de gestión	Logros y Resultados esperados
MINTIC - Ministerio de las Tecnologías de la información y Comunicaciones	Información acerca de la ejecución de los planes, servicios, ejes temáticos, marco estratégico de TI y Gobierno Digital, así como la socialización de políticas de gobierno frente al tema de tecnología.	Colaboración y recursos para la implementación de las políticas establecidas por el ente, en relación con el componente de Seguridad y privacidad de la información de acuerdo con la estrategia de Gobierno Digital.	Lineamientos Normativa.	Cumplimiento normativo de Gobierno Digital.
Policía Nacional – DIJIN	Informe de incidentes presentados en el Instituto para su gestión siempre que sea necesario.	Suministro de evidencia digitales a la DIJIN, para el análisis forense por parte de este	Manual Políticas de Seguridad de la Información.	Respuesta oportuna a incidentes de Seguridad de la Información que contemplan

		Ente		análisis forense.
Contraloría	Información acerca de los procesos que soliciten para su gestión.	Cumplimientos normativos.	Cumplimiento requisitos fiscales.	Evitar sanciones o hallazgos por entes de control.
Procuraduría	Información acerca de los procesos que soliciten para su gestión.	Cumplimientos normativos.	Cumplimiento de requisitos sancionatorios	Evitar sanciones o hallazgos por entes de control.
Fiscalía	Proceso de Cadena de custodia cuando se requiera	Solicitud de cadena de custodia cuando lo requiera un incidente de seguridad de la información.	Manual Políticas de Seguridad de la Información.	Respuesta oportuna a incidentes de Seguridad de la Información.
Alcaldías	Cooperación ante eventos catastróficos o de continuidad del negocio.	Cumplimientos normativos en continuidad del negocio.	Manual Políticas de Seguridad de la Información.	Apoyo para la implementación y ejecución de los planes de continuidad del negocio.
Gobernaciones	Cooperación ante eventos catastróficos o de continuidad del negocio.	Cumplimientos normativos en continuidad del negocio.	Manual Políticas de Seguridad de la Información.	Apoyo para la implementación y ejecución de los planes de continuidad del negocio.

Aliados estratégicos

Parte interesada	**Necesidades**	**Expectativas**	**Requisitos en el sistema de**	**Logros y Resultados**

			gestión	**esperados**

CSIRT - PONAL - Equipo de Respuesta a Incidentes de Seguridad Informática	Informes de alerta de ataques que se están presentando a nivel mundial y local, y que puedan afectar a alguna entidad estatal colombiana.	Comunicación y colaboración permanente sobre el manejo de incidentes que afecten la seguridad de la información.	Manual Políticas de Seguridad de la Información.	Respuesta oportuna a incidentes de Seguridad de la Información
CCP - Centro Cibernético Policial	Ciberseguridad Ciudadana.	Investigación y Judicialización.	Manual Políticas de Seguridad de la Información	Respuesta oportuna a incidentes de Seguridad de la Información.
COLCERT	Ciberseguridad de Infraestructuras Críticas del país.	Coordinación de emergencias ante incidentes.	Manual Políticas de Seguridad de la Información	Respuesta oportuna a incidentes de Seguridad de la Información
CCOCI - Comando Conjunto de Operaciones Cibernéticas	Ciberdefensa de Infraestructuras Críticas Cibernética Nacional de Colombia.	Participación del MVCT de las convocatorias de este ente para la implementación de controles a las infraestructuras críticas.	Manual Políticas de Seguridad de la Información	Ser parte del Plan Nacional de Protección de Infraestructura Crítica Cibernética del país.
SIC - Superintendencia de Industria y comercio	Registro de Base de datos en el marco de la Ley 1581 de 2012.	Cumplimientos normativos.	Cumplimento de requisito legal.	Evitar sanciones o hallazgos por entes de control.

11. ESTRUCTURA DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La política de seguridad de la información es la declaración general que representa la posición del Ministerio de Vivienda, Ciudad y Territorio con respecto a la protección de los activos de información, con la implementación de un sistema de gestión de seguridad de la información.

El Ministerio de Vivienda, Ciudad y Territorio debe contar con políticas, procedimientos y tecnologías apropiadas para proteger los mecanismos de procesamiento, almacenamiento y comunicación donde están almacenados y soportados sus servicios de consulta, registro, validación y realización de trámitesen sus sistemas de información, archivos y bases de datos, contando con funcionarios competentes y comprometidos con una cultura de seguridad reflejada en la aceptación y aplicación de las directrices establecidas.

Con la implementación de las políticas de seguridad de la información, el Ministerio busca dar cumplimiento a las disposiciones legales emitidas por MINTIC a través del decreto 1008 del 14 de junio de 2018 el cual da los lineamientos en la estrategia de Gobierno Digital y contar con la metodología de gestión de riesgos de la Norma ISO 31000, utilizada en la gestión del sistema de calidad, como herramienta para actuar proactivamente ante la presencia de situaciones que puedan afectar la continuidad de los procesos del Ministerio.

Las políticas de seguridad de la información del MVCT se dividen en tres niveles, los cuales se definen según su orden de importancia en:

11.1.1 Primer nivel

Corresponde a la **Política de Seguridad de la información**, la cual es una directriz global que establece qué y por qué se quiere proteger. Su definición está alineada con las normas internacionales ISO 27001:2013 para gestionar la seguridad de la información y con el PETI –plan estratégico de TI del Ministerio de Vivienda, Ciudad y Territorio y está definida en la resolución mediante la cual se establece el SGSI en el Ministerio.

11.1.2 Segundo nivel

Corresponde a las **Políticas Generales de Seguridad de la información**, las cuales establecen las responsabilidades generales aplicables a todos los funcionarios, contratistas del Ministerio de Vivienda, Ciudad y Territorio, así como a los terceros que tienen vinculación con el Ministerio, en lo que respecta al uso adecuado de los activos de información para la gestión de la información.

11.1.3 Tercer nivel

Corresponde a **Políticas Específicas de Seguridad de la información**, enfocadas a grupos, servicioso actividades particulares. Estas políticas o lineamientos resumen los aspectos más relevantes en seguridad de la información para el Ministerio.

12. POLITICAS DE SEGURIDAD DE LA INFORMACIÓN DEL MVCT

12.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El Ministerio de Vivienda, Ciudad y Territorio apoya la implementación del sistema de gestión de seguridad de la información (SGSI), en cumplimiento de los requisitos legales y regulatorios, mediante el establecimiento de criterios, lineamientos, directrices, controles físicos y digitales, asignación de responsabilidades generales y específicas que permitan cumplir con una cultura de seguridad de la información, previniendo incidentes a través de la gestión de riesgos de seguridad y privacidad de la información y seguridad digital, frente a amenazas internas o externas, deliberadas o accidentales, que garanticen y preserven la confidencialidad, integridad y disponibilidad de la información, de todos los funcionarios, contratistas y grupos de interés de la Entidad con el fin de prestar servicios con calidad y recurso humano comprometido a toda la población Colombiana.

12.2 POLITICAS GENERALES DE SEGURIDAD DE LA INFORMACION

12.2.1 Política de dispositivos móviles

El Ministerio de Vivienda, Ciudad y Territorio, a través de la Oficina de Tecnologías de la Información y las Comunicaciones, permite el uso de dispositivos móviles al interior de sus instalaciones siempre y cuando se cumplan los lineamientos, controles y demás aspectos frente al uso de estos en la red del Ministerio.

Esta política aplica a todos los dispositivos y equipos móviles de los funcionarios, contratistas o terceros de la entidad que estén autorizados para conectarse a las redes de datos del MVCT y busca garantizar la seguridad de la información cuando se administre, transmita o almacene información del Ministerio en dichos dispositivos y a su vez controlar el acceso a los mismos.

12.2.2 Política de protección de dispositivo propio (BYOD)

Como política general el Ministerio de Vivienda, Ciudad y Territorio autorizará el uso de dispositivos BYOD para el tratamiento de información institucional. El Ministerio determinará mediante sus procedimientos en qué momento se considera viable autorizar el uso de dispositivos personales que no sean propiedad del Ministerio para el tratamiento de la información institucional.

El Ministerio de Vivienda, Ciudad y Territorio, a través de la Oficina de Tecnologías de la Información y las Comunicaciones permite el uso de dispositivos móviles

personales al interior de sus instalaciones siempre y cuando se cumplan los lineamientos, controles y demás aspectos frente al uso de estos en la red del Ministerio.

Esta política define las medidas necesarias para evitar que la información pública reservada o pública clasificada se vea comprometida en su integridad y confidencialidad al ser almacenada en dispositivos de propiedad de funcionarios o contratistas del MVCT. Esta política aplica a todos los dispositivos electrónicos personales tales como teléfonos inteligentes y tabletas, los computadores portátiles que no pertenecen al Ministerio pero que son utilizados por funcionarios y contratistas para acceder o almacenar información. A estos dispositivos se les conoce comúnmente como BYOD (Bring Your Own Device – Trae tu propio dispositivo).

12.2.3 Política de teletrabajo y/o trabajo remoto

EL Ministerio de Vivienda, Ciudad y Territorio, a través del Grupo de Talento Humano, la Oficina de Tecnologías de la Información y las Comunicaciones y demás dependencias que se requieran deberán establecer los lineamientos, controles y demás aspectos frente al teletrabajo y/o trabajo remoto al interior del Ministerio.

Esta política debe ser aplicada por todos los funcionarios y/o contratistas que realicen teletrabajo y/o trabajo remoto.

12.2.4 Política de control de acceso

EL Ministerio de Vivienda, Ciudad y Territorio, a través de los Líderes de los procesos o los responsables de los activos de información deberán establecer controles de acceso sobre los mismos, con el fin de protegerlos contra accesos no autorizados.

Esta política debe ser aplicada por todos los funcionarios, contratistas y terceras partes que por la naturaleza de sus funciones acceden a los activos de información del Ministerio.

12.2.5 Política sobre el uso de controles criptográficos

EL Ministerio de Vivienda, Ciudad y Territorio, a través de la Oficina de Tecnologías de la Información y las Comunicaciones, establecerá controles criptográficos con el fin de proteger y cifrar la información

al momento de almacenamiento y/o transmisión por cualquier medio y proteger la confidencialidad, la autenticidad y/o la integridad de la misma.

12.2.6 Política de escritorio limpio y pantalla limpia

Todos los colaboradores del Ministerio de Vivienda, Ciudad y Territorio deberán

mantener la información objeto de su labor debidamente custodiada y salvaguardada del acceso de personas no autorizadas.

Los puestos de trabajo deberán permanecer organizados y la información clasificada como reservada, deberá guardarse bajo llave o en lugares vigilados mientras el colaborador responsable de la misma no esté trabajando con ella.

En cuanto a la información que se maneja en los equipos del MVCT, los colaboradores deberán conservar la pantalla libre de accesos directos a información del Ministerio.

Esta política debe ser aplicada por todos los funcionarios, contratistas y terceras partes que por la naturaleza de sus funciones acceden a los activos de información del Ministerio.

12.2.7 Política respaldo de la información

El Ministerio de Vivienda, Ciudad y Territorio, debe asegurar que la información con cierto nivel de clasificación, definida en conjunto por la Oficina TIC y las dependencias responsables de la misma, contenida en la plataforma tecnológica del Ministerio, como servidores, dispositivos de red para almacenamiento de información, entre otros, sea periódicamente respaldada mediante mecanismos y controles que garanticen su identificación, protección, integridad y disponibilidad. Adicionalmente, se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado.

Esta política debe ser aplicada por todos los funcionarios, contratistas y terceras partes que por la naturaleza de sus funciones acceden a los activos de información del Ministerio.

12.2.8 Políticas y procedimientos de transferencia de información

El Ministerio de Vivienda, Ciudad y Territorio, debe garantizar la protección de la información.

Cualquier intercambio de información con entes externos debe quedar formalizado mediante un acuerdo de intercambio de información documento que deben firmar las dos partes intervinientes.

Cuando un tercero proponga un anexo o documento que contenga condiciones o clausulas para asegurar el intercambio entre partes, éste podrá sustituir el acuerdo establecido por el Ministerio siempre y cuando este lo acepte.

La Oficina de Tecnologías de la Información y las Comunicaciones deberá establecer las condiciones técnicas que se deben cumplir para el intercambio de información con terceros.

12.2.9 Política de desarrollo de software

Cuando el Ministerio de Vivienda, Ciudad y Territorio, desarrolle software o contrate el desarrollo de software con proveedores, deberá considerar los lineamientos generales para el desarrollo, mantenimiento y adquisición de software, que defina la Oficina TIC con el fin de adoptar los controles de seguridad en el desarrollo del software.

La única dependencia que puede contratar o desarrollar software (aplicaciones o sistemas de información) en el Ministerio de Vivienda, Ciudad y Territorio es la Oficina de Tecnologías de la Información y las Comunicaciones.

12.2.10 Política de seguridad para las relaciones con proveedores

Los terceros o proveedores del Ministerio de Vivienda, Ciudad y Territorio deberán acatar y cumplir con todos las políticas y lineamientos de seguridad de la información que el marco del desarrollo de la actividad contratada tenga aplicabilidad.

Está política aplica a proveedores de servicios del Ministerio de Vivienda, Ciudad y Territorio y contratistas y busca preservar los niveles de seguridad y privacidad de los activos de información del MVCT, cuando se autorice el acceso o administración por parte de proveedores de servicios o contratos de prestación de servicios.

12.2.11 Política de manejo de información de los servidores de la entidad frente a terceros

Todos los servidores públicos que, dentro del ámbito de sus competencias, deban viajar y atender ciudadanos y en el ejercicio de brindar información a terceros se les solicite información personal de otros funcionarios de la entidad, esta información no puede ser suministrada sin el previo y explicito conocimiento y autorización del propietario de la información.

13. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

Las numeraciones de las políticas específicas de seguridad de la información conservan su numeración de acuerdo con el anexo A de la norma ISO: 27001:2013

A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

A.6.1 Organización interna

- Los roles y responsabilidades para la seguridad de la información son los dispuestos en el numeral 7 Roles y responsabilidades de la seguridad de la información del presente manual. El Líder del sistema de seguridad de la información debe dar a conocer los roles y responsabilidades a todos los colaboradores del Ministerio.
- La información deberá 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 MVCT.
- El Líder del sistema de seguridad de la información deberá mantener contacto con las autoridades nacionales e internacionales en materia de seguridad de la información, y los boletines que estas entidades emitan deberán ser publicados en el micrositio de SGSI en la intranet del MVCT. Estos deberán ser divulgados a los colaboradores del Ministerio.
- El Líder del SGSI deberá mantener los contactos apropiados con los grupos de interés especial u otros foros de seguridad 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.

A.6.2 Dispositivos móviles

- La Oficina TIC, deberá establecer lineamientos para el uso y control de dispositivos móviles (Computadores Portátiles, Tablet, Smartphone), que permita orientar a los funcionarios del Ministerio y a terceros que requieran acceder a los servicios de tecnología.
- Se debe mantener un control formal de los dispositivos móviles conectados a las redes telecomunicaciones e infraestructura de tecnología de información y comunicaciones del MVCT.
- La autorización de la conexión de dispositivos móviles debe considerar las restricciones de acceso a la información y los privilegios de uso de información del usuario.
- El Grupo de Recursos Físicos debe tener un control para el ingreso y salida de las instalaciones del Ministerio (bitácoras o registro en sistemas de información).
- El Grupo de Recursos Físicos, deberá suministrar guayas de seguridad para los equipos portátiles institucionales con el fin de evitar el robo de los mismos.
- En caso de pérdida o robo del dispositivo móvil el funcionario, contratista o tercero responsable del mismo, deberá comunicarlo inmediatamente a su Jefe y debe reportar este hecho como un incidente de seguridad al Jefe de la Oficina TIC y al Jefe del Grupo de Recursos Físicos, para que sea atendido.
- La Oficina TIC, deberá contar con una herramienta que permita hacer borrado seguro de la información del Ministerio en caso de pérdida o robo del dispositivo móvil institucional.
- El Grupo de Recursos Físicos debe establecer un procedimiento ante pérdida de dispositivos móviles asignados a los colaboradores.
- Los Smartphone, propiedad del Ministerio asignados por el Grupo de Recursos Físicos, deberán disponer de sistemas de autenticación de usuarios (Patrón de

desbloqueo, código de seguridad, clave o registro biométrico).

- Los colaboradores (funcionarios y/o contratistas) son responsables de la custodia de los dispositivos móviles y se harán responsables dentro y fuera de las instalaciones de los mismos, igualmente, de la información almacenada en estos, por tal razón deberá desarrollar mecanismos para el respaldo de información periódicamente, de ser necesario solicitar apoyo a la Oficina TIC.
- Para los dispositivos móviles propiedad del MVCT, la Oficina TIC deberá hacer la disposición de herramientas de ofimática, antivirus, medios de almacenamiento virtual (almacenamiento en nube), y las que se requieran siempre y cuando estas hagan parte de la línea base de software del Ministerio, igualmente la restricción de instalación de software por parte del usuario final.
- La Oficina TIC debe sensibilizar a los propietarios o responsables de los dispositivos móviles acerca de los cuidados y responsabilidades que tienen sobre cada uno de los componentes de procesamiento electrónico de información. (Portátiles, Tablet, IPad, teléfonos inteligentes, entre otros).
- Todos los dispositivos móviles propiedad del Ministerio que almacenen información deben estar protegidos contra software malicioso y ser actualizado regularmente.
- Los dispositivos móviles propiedad del MVCT deberán cumplir con la política de control de acceso, y los colaboradores que deseen configurar sus dispositivos personales deberán acogerse a las políticas de monitoreo del dispositivo móvil, sin que esto incurra en una violación a la privacidad del colaborador.
- Los colaboradores deberán evitar la descarga de contenidos sospechosos o que procedan de fuentes no verificables (tanto a través de correo, como de navegación) en los dispositivos móviles y equipos portátiles entregados por el Ministerio.
- Los colaboradores que tengan asignado un dispositivo móvil del MVCT serán responsables de hacer buen uso de la información del Ministerio que sea almacenada en estos dispositivos teniendo en cuenta que éste es para uso exclusivo de sus funciones u obligaciones contractuales.
- Los colaboradores que tengan asignado un dispositivo móvil propiedad del MVCT no están autorizados a cambiar la configuración, desinstalar software, formatear o restaurar de fábrica el equipo asignado. Únicamente debe aceptar y aplicar las actualizaciones requeridas por el equipo.

A.6.2.1 Protección de dispositivo propio (BYOD)

- Los Líderes de los procesos, los Jefes de Oficina, los Directores de Dependencia deben determinar en qué procesos y/o dependencias y bajo qué circunstancias se autorizará el uso de dispositivos que no pertenecen a la entidad (BYOD) para almacenar o procesar información Institucional pública reservada o información pública clasificada, así como la aplicación de las políticas de seguridad requeridas para la información que se almacene y gestione en el dispositivo personal del funcionario o contratista.
- Los Líderes de los procesos deben evaluar los riesgos asociados a la divulgación de información pública reservada o información pública clasificada antes de

autorizar el uso de los BYOD.

- Validar si se permite la conexión de dispositivos personales o terceros
- La Oficina TIC, mediante la mesa de servicio deberá realizar una verificación del dispositivo para que cumpla como mínimo con lo siguiente:
- El dispositivo deberá contar con el Sistema Operativo licenciado.
- El dispositivo deberá contar con un Software Antivirus Actualizado.
- El dispositivo no deberá tener software instalado que le permita saltarse los controles de seguridad del Ministerio.
- El dispositivo deberá permanecer actualizado con las últimas actualizaciones de seguridad.
- La conexión y uso de dispositivos móviles en la red del Ministerio debe ser autorizado por la Oficina TIC.
- Se debe mantener un registro y control formal de los dispositivos móviles autorizados a conectarse a las redes del MVCT
- Los dispositivos personales que se conecten al directorio activo, deberán hacer parte de un grupo denominado Terceros.
- El funcionario o contratista tercero al que se autorice el uso de su dispositivo personal debe garantizar bajo compromiso de confidencialidad que la información pública reservada o información pública clasificada correspondiente a sus labores asignadas será almacenada de forma aislada a la información personal que guarde en su dispositivo.
- Todo dispositivo BYOD autorizado para almacenar información de la entidad debe cumplir con la reglamentación vigente en materia de uso de software legal. El usuario es enteramente responsable de contar con todo el software de su dispositivo debidamente licenciado.
- La Oficina TIC, pueden realizar revisiones a los equipos BYOD para certificar que están cumpliendo con las políticas de seguridad de la información, las revisiones preservaran el derecho fundamental a la intimidad del usuario del BYOD y las normas sobre Protección de Datos de carácter personal.
- El propietario del dispositivo BYOD debe aplicar todas las medidas de seguridad razonables que estén a su alcance para preservar la integridad, confidencialidad y disponibilidad de la información que se encuentre en su dispositivo personal.
- El propietario del dispositivo BYOD debe aplicar medidas de seguridad que minimicen la pérdida o hurto del mismo.
- El propietario del dispositivo debe informar sin demoras injustificadas a la Oficina TIC, y a la autoridad competente el robo o pérdida de su dispositivo. El MVCT gestionará la pérdida o divulgación de información almacenada en los dispositivos BYOD, mediante el procedimiento de gestión de incidentes de seguridad de la información.
- La información clasificada como publica reservada o publica clasificada deberá almacenarse en los repositorios establecidos por la Oficina TIC "OneDrive y servidores de archivo", no deberá guardarse en los discos duros del BYOD o en otros dispositivos personales.

A.6.3 Teletrabajo o trabajo en casa

En función de la ley 2088 de 2021

- Los criterios y condiciones para ejercer la modalidad de teletrabajo o trabajo remoto deberán ser definidos de forma integral por el comité de Teletrabajo, teniendo como base la normativa legal vigente mediante la formalización y/o actualización de procedimientos que incluyan los aspectos de seguridad de la información.
- Los colaboradores que requieran acceder a los recursos informáticos del MVCT fuera de las instalaciones del mismo deberán realizarlo a través de una conexión de red virtual privada (VPN) o por medio de la plataforma de nube de Office 365 para el manejo adecuado de la información, previa autorización del Jefe inmediato o Supervisor de contrato y del Jefe de la Oficina TIC.
- Las conexiones de la modalidad de teletrabajo o trabajo remoto, deberán ser monitoreadas y supervisadas según el perfil de usuario y/o asignación roles y privilegios, igualmente verificar la desactivación de los accesos una vez el funcionario o contratista no tenga vinculación con la entidad.
- Antes de su aprobación todo acceso a servicios de teletrabajo debe ser sometido a una evaluación de riesgos de seguridad de la información y de seguridad y salud en el trabajo.
- Los responsables de los procesos que autoricen servicios de teletrabajo deben realizar una evaluación de riesgos digitales sobre los accesos solicitados y formular las recomendaciones de controles de seguridad necesarios para la implementación del acceso. En caso de identificar riesgos que no son aceptables se deberá notificar al Jefe de la Oficina TIC y al peticionario del servicio la imposibilidad de activar los servicios de teletrabajo en las condiciones presentadas en la solicitud.
- Para el acceso al teletrabajo o trabajo remoto se deben tener en cuenta las necesidades técnicas y tecnológicas que garanticen que el funcionario o el colaborador, cuente con las herramientas necesarias para poder realizar su trabajo, así como las configuraciones de acceso seguro, los medios y horarios que solicite el responsable del proceso manteniendo en todo momento los principios de eficiencia, eficacia y uso racional de los recursos del Estado.
- Los servicios de teletrabajo o trabajo remoto deben ser implementados con controles del sistema de gestión de seguridad de la información.
- Cualquier dispositivo que se emplee para las actividades de teletrabajo deberá cumplir con los requisitos y controles de seguridad que defina la Oficina de TIC.
- Las conexiones a servicios de teletrabajo deben permanecer cifradas con los controles de seguridad del SGSI y utilizando conexiones seguras o redes privadas entre el lugar dónde se realiza el teletrabajo o trabajo remoto y los sistemas de información del MVCT.
- El acceso a los servicios de teletrabajo o trabajo remoto, se deben usar para el cumplimiento de las funciones asignadas y para el cumplimiento de la misión y objetivos del Ministerio, cualquier uso diferente está expresamente prohibido.
- Los funcionarios y/o contratistas que realicen teletrabajo o trabajo remoto, son responsables de reportar a la mayor brevedad la posible la pérdida o hurto de los equipos y/o dispositivos móviles usados para teletrabajo o el trabajo remoto y

que se encuentren bajo su responsabilidad.

- La estación de trabajo del colaborador debe cumplir con la reglamentación en cuanto a uso de software legal.
- La estación de trabajo del colaborador debe tener activo el firewall y debe contar con software de protección contra código malicioso.
- Los sistemas operativos de los computadores desde donde se realicen actividades de teletrabajo o trabajo en casa deben estar actualizados y contar con controles que mitiguen las vulnerabilidades de seguridad.
- La Oficina TIC debe asignar el acceso únicamente a la información, servicios y sistemas de información necesarios para la realización de las actividades a cargo del empleado que solicita el acceso al teletrabajo.
- Una vez el colaborador retorne a las instalaciones del Ministerio es responsabilidad del Jefe inmediato informar a la Oficina TIC, para que le sean modificados los accesos concedidos.

A.7 SEGURIDAD DE LOS RECURSOS HUMANOS

A.7.1 Antes de asumir el empleo

-
- El Grupo de Talento Humano deberá 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 MVCT y los que dicte la Función Pública.
- El Grupo de Contratos deberá definir una lista de verificación que contengan los aspectos necesarios para la revisión de los antecedentes, certificaciones académicas y laborales entre otras del personal a contratar por prestación de servicios de acuerdo con lo que dicta la Ley y la reglamentación vigente.
- Los procesos de selección de personal de planta y procesos contractuales deberán contener la autorización para el tratamiento de los datos personales de acuerdo con la Política de tratamiento de datos personales del MVCT y de acuerdo a lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios.
- Los documentos de verificación deberán reposar en la historia laboral o carpeta contractual del colaborador.
- El Grupo de Talento Humano y el Grupo de Contratos, deberán establecer los mecanismos o controles necesarios para proteger la confidencialidad y reserva de la información contenida en las historias laborales y expedientes contractuales.

A.7.2 Durante la ejecución del empleo

- El Grupo de Contratos deberá definir los términos y condiciones del contrato, en los cuales se establecerá las obligaciones del contratista en materia de seguridad de la información, las leyes de propiedad intelectual, de protección de datos personales, de transparencia y acceso a la información pública.
- El Grupo de Talento Humano, deberá dar a conocer a los colaboradores los

términos y condiciones de empleo o contrato y especificar los roles y las responsabilidades u obligaciones en materia de la seguridad de la información y aclarar que estas se extienden más allá de los límites del MVCT y del horario normal de trabajo o de ejecución del objeto contractual.

- El Grupo de Contratos deberá incluir en el pliego de condiciones o estudios previos para la contratación de terceras partes, las obligaciones referentes a las políticas, lineamientos y directrices en materia de seguridad de la información que dicte el MVCT.
- El Grupo de Talento Humano y el Grupo de Contratos, deberán hacer firmar un documento de compromiso de confidencialidad de la información que contenga como mínimo el cumplimiento de las políticas institucionales y normatividad vigente a todos los funcionarios del MVCT, cualquiera sea su situación contractual, la dependencia a la cual pertenezca y las tareas que desempeñe, dicho documento debe reposar en la historia laboral o expediente contractual según sea el caso.
- El Grupo de Talento Humano, conjuntamente con la Oficina TIC darán a conocer el manual de políticas de seguridad de la información a los colaboradores del MVCT.
- Una vez formalizado el proceso de vinculación, el grupo de talento humano y el grupo de contratos autorizaran la creación de la cuenta de usuario, La solicitud de creación es responsabilidad de dependencia a la cual se vinculará el funcionario.
- El Grupo de Talento Humano, el Grupo de Contratos, el Supervisor del Contrato o el Jefe inmediato deberá informar a la mesa de servicios sobre las novedades del colaborador y la acción a tomar (bloqueo o desbloqueo) de los recursos tecnológicos.
- El Ministerio deberá incluir dentro de los programas de inducción y/o reinducción, sesiones de capacitación y sensibilización del sistema de gestión de seguridad de la información para los funcionarios y contratistas.
- La Oficina TIC, diseñará e implementará en el plan de uso y apropiación estrategias de cultura y apropiación referentes a seguridad de la información.
- Todos los funcionarios, contratistas y terceros del MVCT, deberán almacenar la información de la operación, únicamente en los repositorios autorizados el Ministerio.

Proceso disciplinario por incumplimiento de las políticas de seguridad de información

- El incumplimiento de las políticas de seguridad de la información del MVCT por parte de los funcionarios, contratistas y terceros de la Entidad, conllevará a incurrir en sanciones disciplinarias o legales según corresponda.
- El Grupo de Control Interno Disciplinario debe aplicar las normas y leyes para investigar y sancionar disciplinariamente los casos en que se presenten usos de información y tecnología que violen los términos y condiciones de la política de seguridad de la información del MVCT y los acuerdos firmados por los funcionarios.
- Con la implementación de políticas en seguridad de la información el Ministerio

da cumplimiento a las disposiciones legales y regulatorias emitidas por los diferentes organismos estatales, a fin de contar con una metodología de gestión de riesgos como herramienta para actuar proactivamente ante la presencia de situaciones que puedan afectar la continuidad de los procesos del Ministerio.

- Todos los funcionarios del MVCT (de carrera administrativa, de libre nombramiento y remoción, provisionales, contratistas, proveedores, terceros, entre otros) que tengan acceso a los sistemas de información, recursos informáticos y demás activos de información del Ministerio, deben cumplir con la Política General de Seguridad y Privacidad de la Información y Seguridad Digital.
- El incumplimiento de las políticas, lineamientos y/o procedimientos de seguridad, para los servidores públicos constituye falta disciplinaria conforme a lo señalado en los numerales 4 y 5 del artículo 34 y numerales 16 y 43 del artículo 48 de la ley 734 de 2002 y las normas que las sustituyan o modifiquen.

  Artículo 34 Son deberes de todo servidor público:
  "*4. Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función en forma exclusiva para los fines a que están afectos."*
  "5. Custodiar y cuidar la documentación que, por razón de su empleo, cargo o función, conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos."

  Artículo 48. Son faltas Gravísimas las siguientes:
  "16. Atentar con cualquier propósito, contra la inviolabilidad de la correspondencia y demás formas de comunicación, u obtener información o recaudar prueba con desconocimiento de los derechos y garantías constitucionales y legales".

  "43. Causar daño a los equipos estatales de informática, alterar, falsificar, introducir, borrar, ocultar o desaparecer información en cualquiera de los sistemas de información oficial contenida en ellos y en los que se almacene o guarde la misma, o permita el acceso a ella a personas no autorizadas."
-
- Los funcionarios que incumplan la política de seguridad adoptada mediante Resolución 0331 del 28 de junio de 2021, dependiendo de la gravedad del incidente se podrán ver involucrados en un proceso disciplinario con las consecuencias que de ellas se deriven, según lo establecido en el Código Disciplinario Único, cuyas sanciones pueden ser desde una amonestación escrita a la hoja de vida hasta la destitución e inhabilidad general.
- Los contratistas sean personas naturales o jurídicas que incumplan la política de seguridad, pueden verse afectados con la terminación de su contrato dependiendo de la gravedad del incidente de acuerdo con las condiciones que en él se han establecido como también verse incursos en una investigación penal.
- El Grupo de Control Interno Disciplinario es la dependencia competente para realizar una investigación disciplinaria según lo establecido en el Ley Disciplinaria

vigente una vez agotado el procedimiento definido para ello.

- En caso de que se compruebe algún incumplimiento total o parcial de las políticas de seguridad de la información, se dará lugar a sanciones disciplinarias que establezca la Ley.
- Una vez se determine una situación de un posible incumplimiento de las políticas de seguridad de la información el procedimiento a seguir se describe a continuación:
- Cuando un funcionario, contratista o tercero, incurra en un incumplimiento de las políticas de seguridad de la información y el impacto del incidente sea de menor grado, el Líder del Sistema de Gestión de Seguridad de la Información llamará la atención al autor del hecho sin necesidad de acudir a formalismo procesal alguno el cual no generará antecedente disciplinario.
- Si el Líder de seguridad de información observa que el incumplimiento generó una grave afectación a uno o varios activos de información, lo comunicará al Grupo de Control Interno Disciplinario para que proceda a iniciar la respectiva investigación disciplinaria y determine la sanción a que haya lugar para el funcionario de acuerdo con la Ley Disciplinaria.
- Si el Líder de seguridad de información observa que un contratista o tercero generó una grave afectación a uno o varios activos de información, lo comunicará al Supervisor del contractual para que a través de este se inicien las acciones administrativas correspondientes y proceda a informarlo a la entidad penal competente.

A.7.3 Terminación y cambio de empleo

-
- El supervisor del contrato o a quien delegue deberá custodiar la información del MVCT bajo la responsabilidad de los contratistas en caso de terminación anticipada, definitiva, temporal o cesión del contrato.
- El Jefe inmediato o a quien delegue deberá recoger y custodiar la información del MVCT bajo la responsabilidad de los funcionarios en el caso de retiro, investigación, inhabilidades, o cambio de funciones.
- El Grupo de Talento Humano y el Grupo de Contratos o a quienes se deleguen deberán informar a la Oficina TIC a través de la mesa de servicios, cualquier novedad de desvinculación administrativa, laboral o contractual del colaborador o cambio de rol; una vez notificada la novedad la Oficina TIC 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 o de servicio (ejemplo: info@minvivienda.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 suintegridad. Se deben inactivar los accesos biométricos de los sistemas de control de acceso.
    - Emitir comunicado a los proveedores y demás personal con el que el colaborador tenga contacto, indicándole que esa persona ya no labora en

el MVCT e indicar quién asumirá sus funciones o responsabilidades.

- Adicionalmente en desvinculación:
  - Para el buzón de correo electrónico este pasara a un estado de "Litigation" una vez se dé por terminada la vinculación con el Ministerio.
  - 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.
  - Se deben inactivar todos los accesos a los sistemas de información.
  - Se debe solicitar la devolución del carné o cualquier distintivo de autenticación o prenda de vestir, que lo acredita como colaborador del MVCT.
- El Grupo de Talento Humano, deberá comunicar a los funcionarios y contratistas, las responsabilidades respecto a seguridad de la información que se derivan de la terminación o cambio de empleo.
- El funcionario, contratista y/o proveedor deberán entregar todos los activos de información según como lo determina el procedimiento de terminación del empleo, así mismo el proceso de entrega del cargo o separación temporal del mismo, y los informes de supervisión de contrato según el caso que aplique.
- Los funcionarios o contratistas podrán solicitar copia de su buzón electrónico hasta antes de noventa días (90), una vez terminada su vinculación con el Ministerio y deberán suministrar los medios de almacenamiento necesarios para la entrega.

A.8 GESTIÓN DE ACTIVOS

A.8.1 Responsabilidad por los activos

- El Líder del SGSI o a quien este delegue deberá aplicar y mantener actualizada la documentación para el levantamiento y actualización de los activos de información del MVCT.
- La identificación, clasificación y valoración de activos del MVCT, deberá ser realizado por los Líderes de proceso, en el formato de registro de activos de información, de acuerdo con lo definido en la guía para la gestión de activos de información del MVCT. Este proceso deberá actualizarse anualmente o previo a los cambios normativos vigentes.
- Los Líderes de los procesos del MVCT, serán los propietarios de los activos de información identificados para sus procesos.
- Los Líderes de los procesos deben establecer los controles sobre los activos de información.
- El Líder del SGSI o a quien este delegue, deberá remitir el consolidado del levantamiento de activos de información, al Profesional que lidera la estrategia de la ley de transparencia y acceso a la información pública y la estrategia de gobierno en línea o a quien haga sus veces, con el objetivo de ser analizada, realimentada, actualizada y publicada de acuerdo a la normativa vigente colombiana.

- Los funcionarios, contratistas y usuarios de los activos de información y de la información del MVCT deben:
- Aceptar y cumplir las políticas de seguridad de la información establecidas en el Ministerio.
- Proteger contra pérdida, modificaciones y acceso no autorizados a los activos de información del Ministerio.
- Comprender y aceptar sus responsabilidades frente al acceso a los diferentes sistemas de información que se tienen o administran en el Ministerio.
- Los Líderes de proceso del MVCT deberán realizar la respectiva aceptación de los activos de información del proceso a su cargo, con el fin de establecer posteriormente los riesgos de seguridad digital a los que estos se vean expuestos.
- La Oficina TIC, debe establecer lineamientos para el uso y acceso a los recursos de tecnología del Ministerio "correo electrónico, internet office 365 entre otros".
- En caso de que un colaborador deba hacer uso de equipos ajenos al MVCT, estos deberán cumplir con la legalidad del software instalado, antivirus licenciado, actualizado y solo podrá conectarse a la red del MVCT una vez esté avalado por la Oficina TIC.
- El único servicio de correo electrónico autorizado para el manejo de la información institucional en el MVCT es el que cuenta con el dominio @minvivienda.gov.co.
- Las firmas de documentos oficiales que reposan en expedientes, y que se constituyen como activos de información de acuerdo con 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 digitalizadas o escaneadas.
- l MVCT se reserva el derecho de monitorear los accesos y el uso de los buzones de correo institucionales, de todos sus funcionarios o contratistas, además podrá realizar copias de seguridad en cualquier momento, así como limitar el acceso temporal o definitivo a todos los servicios y accesos a sistemas de información del Ministerio o de terceros operados en el mismo por solicitud expresa del Ministro, Viceministros, Secretario General, Jefes de Oficina, Directores, Subdirectores y Coordinadores de Grupo a la Oficina TIC.
- Con el fin de mitigar la suplantación de la identidad de correos electrónicos personales, se prohíbe suministrar acceso directo a los buzones de correo asignado a otro colaborador.
- Para los buzones compartidos el responsable de este debe solicitar a la mesa de servicio el acceso a los colaboradores que el defina.
- No se permite el almacenamiento en los equipos de cómputo y medios de almacenamiento propiedad del MVCT, el almacenamiento de archivos de multimedia (Audio, video, Imágenes), programas ejecutables, o cualquier tipo de archivo que no sea de carácter institucional.
- Únicamente se permitirá el acceso a las aplicaciones y sistemas de información autorizados por el Ministerio, de esta manera evitar la ejecución de software no licenciado el cual atente contra los derechos de autor y propiedad intelectual según como lo regula la ley.
- El acceso a los documentos físicos y digitales estará determinado por las normas

relacionadas con el acceso y las restricciones a los documentos públicos, a la competencia del área o dependencia específica y a los permisos y niveles de acceso de los funcionarios y contratistas determinadas por los Jefes de área o dependencia.

- Para la consulta de documentos adjuntos en el software de gestión documental, se establecerán privilegios de acceso a los funcionarios y/o contratistas de acuerdo con el desarrollo de sus funciones y competencias. Dichos privilegios serán establecidos por el Jefe o Director del área, quien comunicará al Grupo encargado de la administración del software.
- EL MVCT debe realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los funcionarios y/o terceros. Así mismo, puede inspeccionar, registrar y evaluar las actividades realizadas durante la navegación, de acuerdo con la legislación nacional vigente.
- La instalación de cualquier tipo de software o hardware en los equipos de cómputo del MVCT es responsabilidad de la Oficina TIC, y por tanto son los únicos autorizados para realizar esta labor. Así mismo, los medios de instalación del software deben ser los proporcionados por el MVCT a través de esta oficina.
- La Oficina TIC debe definir y actualizar, de manera periódica, la lista de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios. Así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.
- La conexión a redes inalámbricas externas para usuarios con equipos portátiles que estén fuera de la oficina y que requieran establecer una conexión a la infraestructura tecnológica del MVCT, deben utilizar una conexión bajo los esquemas y herramientas de seguridad autorizados y establecidos por la Oficina TIC.
- Sólo personal autorizado puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información del MVCT;
- conexiones establecidas para este fin, deben utilizar los esquemas y herramientas de seguridad y administración definidos por la Oficina TIC.
- Los colaboradores y terceras partes deberán devolver todos los activos de información del MVCT que se encuentran en su poder a la terminación de su empleo, contrato, convenio o acuerdo.
- Cuando sede de baja un equipo de cómputo de los inventarios por cualquier motivo, se deberá realizar un respaldo de la información que en él se encuentre a través de la mesa de servicios. la Oficina TIC debe realizar el borrado seguro de la información que contengan los medios de almacenamiento con el fin de propender que la información del MVCT contenida en estos medios no se pueda recuperar.
- Cuando se realice el traslado de equipos de cómputo a otros colaboradores, se deberá instalar de nuevo el sistema operativo y los programas de la línea base.
- La única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro será la Oficina TIC, sin embargo, cuando deba realizarse desde y hacia el almacén será el Grupo de Recursos Físicos, con el fin

de llevar el control individual de inventarios. En tal virtud, toda reasignación de equipos deberá ajustarse a los procedimientos y competencias de la gestión de bienes del Ministerio.

A.8.2 Clasificación de la información

La Oficina TIC deberá apoyar al Grupo de Atención al Usuario y Archivo los cuales desarrollarán los lineamientos para la clasificación de la información teniendo en cuenta lo siguiente:

- Los propietarios de la información son los encargados de realizar la clasificación de la información.
- El MVCT a través del Grupo de Atención al Usuario y Archivo definirá los tipos de niveles adecuados para clasificación de la información de acuerdo con su sensibilidad donde se valorarán confidencialidad, integridad y disponibilidad de la información. Estos niveles deberán ser oficializados y divulgados a todos los colaboradores.
- Los propietarios y custodios de los activos de información son responsables de monitorear periódicamente la clasificación de sus activos de información y de ser necesario realizar su re- clasificación.
- La información física y digital del MVCT, deberá tener un periodo de almacenamiento que puede ser dado por requerimientos legales o misionales; este periodo deberá ser indicado en las tablas de retención documental y cuando se cumpla el periodo de expiración, toda la información deberá ser eliminada o transferida adecuadamente.
- El MVCT, a través del Grupo de Atención al Usuario y Archivo, la Oficina TIC y el Grupo de Recursos Físicos, deberán establecer los mecanismos necesarios para proteger la información catalogada como Información pública reservada, teniendo en cuenta el medio en que se encuentre.

Manejo de la información.

- Los colaboradores y terceras partes deberán acatar los lineamientos que se definan frente a almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física del MVCT
- La información pública clasificada y pública reservada deberá protegerse incluso en los ambientes de pruebas.
- La información del Ministerio no debe ser divulgada sin contar con los permisos correspondientes, además, ningún funcionario, contratista o proveedor debe copiarla o extraerla en el momento en que se retire del Ministerio o durante su permanencia.
- Los terceros, proveedores u operadores tecnológicos que accedan a la información del Ministerio, no deben hacer copias de la información suministrada por el Ministerio, ni podrán transferirla a otro equipo a través de la red, sin la autorización del dueño de la información
- Los funcionarios y contratistas del MVCT no deben divulgar información pública

clasificada o pública reservada del Ministerio a personas no autorizadas o a entes externos, a menos que se realice por el canal oficialmente establecido y con la aprobación previa del líder de proceso al cual pertenece el activo de información.

A.8.3 Manejo de medios

- El uso de medios de almacenamiento removibles (ejemplo: CDs, DVDs, memorias flash, USBs, Ipods, celulares, cintas) sobre la infraestructura de cómputo del MVCT, deberá ser autorizada por la Oficina TIC.
- La Oficina TIC debe definir políticas o lineamientos para el uso de medios removibles e implementar los controles necesarios para su uso.
- Así mismo, el funcionario se compromete a asegurar física y lógicamente el dispositivo a fin de no poner en riesgo la información del MVCT que este contiene.
- Bajo ninguna circunstancia se dejarán desatendidos los medios de almacenamiento o copias de seguridad de los sistemas de información.
- Todo medio removible deberá ser escaneado mediante antivirus cada vez que se conecte a un equipo de la red del MVCT.
- 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.
- Se prohíbe el uso de medios removibles en lugares de acceso al público que contengan información reservada o clasificada del MVCT.
- El Grupo de Recursos Físicos deberá crear un procedimiento para la disposición final de residuos de aparatos electrónicos.
- La Oficina TIC deberá propender por que el procedimiento de almacenamiento de información (backup- almacenamiento en cintas) cuente con las condiciones para asegurar la confidencialidad, integridad y disponibilidad de la información en custodia.
- Los medios y equipos donde se almacena y procesa información deben mantenerse con las medidas de protección físicas, lógicas y condiciones dadas por los fabricantes, que permitan un adecuado funcionamiento.
- Los medios que requieran ser eliminados, dar de baja o ser reasignados deberán sometidos a un proceso de borrado seguro y demás mecanismos que puedan considerarse, con el fin de evitar la recuperación de la información que alguna vez estuvo contenida en estos medios.
- Los medios removibles que se regresen al almacén para asignarse a otro colaborador o para dar de baja, con el apoyo de la oficina TIC se les deberá ejecutar el procedimiento de borrado seguro o en caso de no poder realizar el borrado seguro validar el procedimiento para la disposición final de residuos de aparatos electrónicos RAEE.

Es requisito realizar el respaldo o copia de la información contenida en el medio removible, previa ejecución del procedimiento de borrado seguro.

- Cuando se requiera transferir un medio de almacenamiento de información del MVCT a otras entidades se deberán establecer un acuerdo entre las partes. Dichos acuerdos deberán dirigirse a la transferencia segura de

información de interés entre el MVCT y las partes.

- El transporte para los medios de almacenamiento deberá contar con las condiciones apropiadas para salvaguardar la integridad, confidencialidad y disponibilidad de la información.
- Toda información propiedad de MVCT de tipo clasificada y/o reservada, almacenada en los diferentes medios y que requieran ser transportados a otras locaciones ajenas a la entidad, deberá cumplir con los lineamientos de seguridad establecidos por el proveedor de servicio.

A.9 CONTROL DE ACCESO

A.9.1 Requisitos del negocio para control de acceso

- El MVCT suministrará a los usuarios las credenciales respectivas 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.
- Es responsabilidad de los colaboradores o terceras partes del MVCT el manejo que se les dé a las credenciales de acceso asignadas.
- El proveedor encargado de la gestión de la plataforma tecnológica del MVCT, debe garantizar el acceso seguro a la misma.
- La conexión remota a la red de área local del MVCT deberá establecerse a través de una conexión VPN suministrada por el Ministerio, la cual deberá ser registrada por la Oficina TIC.
- Las conexiones remotas deberán utilizar los métodos establecidos de autenticación para el control de acceso de los usuarios.
- La Oficina TIC deberá implantar controles para el acceso por redes inalámbricas.
- La Oficina TIC deberá establecer una adecuada segregación de redes, separando los entornos de red de usuarios de los entornos de red de servicios.
- El control de acceso a los datos, información y servicios se deberá basar en el principio del menor privilegio y la necesidad de conocer, lo que implica que no se otorgará acceso a menos que sea explícitamente permitido.
- La Oficina TIC deberá verificar periódicamente los controles de acceso para los usuarios del MVCT 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.
- Los colaboradores y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos del MVCT, deberán contar con el formato solicitud servicios de gestión de los usuarios debidamente autorizado.
- Los equipos personales de los colaboradores que se conecten a las redes de datos del MVCT deberán cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.
- No se podrá utilizar ningún tipo de utilitario para conexión remota a la red interna del MVCT, únicamente se deberá utilizar el autorizado por la Oficina

TIC.

- La Oficina TIC es la responsable de asignar los accesos a plataformas, usuarios y segmentos de red de acuerdo a procesos formales de autorización, los cuales pueden ser evaluados por lasegunda y tercera línea de defensa de acuerdo a lo programado en plan anual institucional y al plan anual de auditorías, respectivamente.
- La autorización para el acceso a los sistemas de información debe ser definida y aprobada porel área propietaria de la información, o quien ésta defina, y se debe otorgar de acuerdo con el nivel de clasificación de la información identificada, según la cual se deben determinar los controles y privilegios de acceso que se pueden otorgar a los funcionarios y terceros eimplementada por la Oficina TIC.
- En caso de conexiones de tipo remoto deben existir mecanismos robustos de autenticación y transmisión segura de datos. Este servicio debe ser restringido solo a usuarios autorizados y específicamente a los recursos que requiera para el cumplimiento de las funciones en el Ministerio, aplicando el principio de "el acceso mínimo permitido".
- Si el Ministerio requiere proporcionar acceso remoto a terceros, deberá contar con controles dered para restringir el uso de servicios no necesarios y limitar los accesos por fecha y hora.
- Todas las conexiones remotas que requieran acceso a la red interna del Ministerio deben pasarforzosamente por un Firewall, el cual proporcione a las redes internas un nivel de seguridad acorde a la sensibilidad de los sistemas, aplicaciones e información disponible en ellas.
- La Oficina TIC es responsable de la administración de redes, debe contar con un procedimiento formal para la autorización de conexiones remotas a los usuarios, el cual incluya por lo menos:
    - Plena identificación del usuario.
    - Justificación del acceso.
    - Sistema e información a la cual requiere acceso.
    - Solicitud formal escrita con la justificación del jefe o coordinador del Área del usuario solicitante dirigida a la Oficina TIC.
- En función de la justificación del usuario para obtener acceso remoto, la Oficina TIC debe determinar el tipo y nivel de acceso que le otorgará, así como establecer un procedimiento de monitoreo periódico de las conexiones y actividades de los usuarios para identificar posibles anomalías en las conexiones o cuentas con inactividad que requieran ser eliminadas.
- Deben existir al menos 3 tipos de acceso remoto:
    - Acceso general: Acceso a correo electrónico corporativo, internet y portal corporativo (intranet) sin aplicaciones.
    - Acceso particular: El mismo acceso que general, más los permisos necesarios para ingresar al sistema o aplicaciones que se justifique y autorice. "Se requiere vpn".
    - Acceso a administradores de sistemas: Acceso a los sistemas e infraestructura asignada según sus funciones. "Se requiere vpn".
- El acceso remoto a terceros no estará permitido a menos que exista una

legítima necesidad justificada para otorgarles el servicio. El usuario externo tendrá que cumplir con un procedimiento formal de autorización con la Oficina TIC.

- Las aplicaciones o sistemas de información nuevos que sean desarrollados al interior del Ministerio o por terceros deberán cumplir como mínimo con los siguientes requisitos deseguridad:
- La autenticación de los usuarios debe hacerse a través del directorio activo.

A.9.2 Gestión de acceso de usuarios

- La Oficina TIC deberá definir un procedimiento para la creación y la cancelación de usuarios enel MVCT, teniendo en cuenta que las identificaciones de los usuarios deberán ser únicas.
- Se deberá definir un estándar para la definición de los usuarios en caso de presentarse homónimos.
- Se deberán deshabilitar las credenciales de acceso a los colaboradores que no tengan ningún vínculo laboral con el MVCT.
- El acceso a la información del MVCT, es otorgado sólo a usuarios autorizados, teniendo en cuenta lo requerido para la realización de sus labores relacionadas con su responsabilidad o tipo de servicio con los privilegios asignados.
- No se deberá configurar el acceso a los recursos tecnológicos a usuarios que no hayan formalizado el proceso de ingreso al MVCT.
- Todo usuario que quiera acceder a servicios o información de la plataforma tecnológica del MVCT, deberá autenticarse.
- Los usuarios deberán cumplir con los lineamientos para la creación y uso de contraseñas.
- El uso de credenciales de usuarios administradores de sistemas operativos, consolas de administración y bases de datos tales como: "root", "adm", "admin", "administrador", "SQLAdmin", "administrator" y "system", entre otros, deberán ser controladas, y vigiladas por elcoordinador del Grupo de Apoyo Tecnológico de la Oficina TIC.
- Todos los colaboradores y terceras partes deberán cumplir las condiciones de acceso ymantener de forma confidencial las contraseñas con la finalidad de preservar el no repudio.
- La Oficina TIC deberá otorgar los privilegios para la administración de recursos tecnológicos, servicios de red y sistemas de información únicamente a aquellos colaboradores o terceros quecumplan dichas funciones.
- La Oficina TIC deberá otorgar cuentas personalizadas con altos privilegios para cada uno de losadministradores de los recursos tecnológicos, servicios de red y sistemas de información, diferentes a los nativos y deberán ser cuentas únicas asociadas al usuario de dominio.
- La Oficina TIC deberá restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deberá permitir el acceso a los colaboradores o terceros autorizados.
- La Oficina TIC deberá deshabilitar los servicios o funcionalidades no utilizadas

de los sistemasoperativos, el firmware y las bases de datos.

- La Oficina TIC deberá mantener un listado actualizado en donde se identifiquen los derechos de acceso privilegiado asociados con cada sistema o proceso, (sistema operativo, sistema de gestión de bases de datos, y cada aplicación del MVCT).
- La Oficina TIC deberá generar registros de auditoria que contengan eventos relacionados de seguridad, teniendo en cuenta criterios tales como nombre de usuario, fechas y hora de evento, tipo de modificación sobre el objeto. Se deberá realizar un respaldo de esta información facilitando la revisión y el análisis de los mismos.
- Los colaboradores de cada dependencia con el privilegio de control total sobre las carpetas compartidas deberán realizar auditorías a las carpetas y subcarpetas, con el fin de establecer controles que permitan validar que solo cuenten con los permisos de acceso los usuarios autorizados.
- La Oficina TIC, deberá tener un listado de las cuentas de servicio que se configuren en el directorio activo y debe establecer un responsable para cada una de ellas.
- La contraseña para la autenticación se deberá suministrar a los usuarios de manera segura, y el sistema deberá solicitar el cambio inmediato de la misma al ingresar por primera vez.
- Se deberán establecer mecanismos para verificar la identidad de un usuario antes de reemplazar la información secreta para la autenticación o proporcionar una nueva o temporal.
- La información secreta para la autenticación por defecto del fabricante se deberá modificar después de la instalación de los dispositivos o del software.
- El retiro de los privilegios de acceso se deberá hacer inmediatamente se realice la solicitud de desactivación de los usuarios.
- Es responsabilidad de los Directores, Subdirectores, Jefes de Oficina o Supervisores de los contratos dar a conocer a la Oficina TIC el retiro, suspensión o cualquier novedad administrativa que se presente con los usuarios del MVCT, esta novedad se deberá reportar a través de la mesa de servicios.
- La Oficina TIC deberá garantizar que la administración de la plataforma tecnológica se realice através de estaciones de acceso privilegiado para cada uno de los administradores.

A.9.3 Responsabilidades de los usuarios

La Oficina TIC establece los siguientes lineamientos para la asignación de información deautenticación secreta teniendo en cuenta lo siguiente:

- Los usuarios son responsables del uso de las contraseñas de acceso que se le asignen parala utilización de los equipos o servicios tecnológicos del MVCT.
- El cambio de contraseña solo podrá ser solicitada por el titular de la cuenta o su Jefeinmediato.

Las contraseñas deberán:

- 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.
- La contraseña deberá tener como mínimo ocho (8) caracteres alfanuméricos.
- La contraseña no deberá contener el nombre de usuario, el nombre real o la sigla MVCT.
- No se deberán usar contraseñas con los nombres de los hijos, esposo, mascotas, fechas de aniversarios, cumpleaños, etc.
- La contraseña deberá ser diferente de otras contraseñas anteriores proporcionadas, es decir las ultimas diez (10) suministradas al dominio no se deberán repetir.
- No se deberán usar las mismas contraseñas de la autenticación para uso personal.
- Las contraseñas deberán estar compuestas por: letras en mayúsculas "A, B, C…", letras en minúsculas "a, b, c…", números "0, 1, 2, 3…", símbolos especiales "@, #, $, %, &, (),
- ¡, ¡, ¿, ¿, <>…" y espacios en cualquier orden.
- Las contraseñas deberán cambiarse obligatoriamente cada 60 días o cuando lo establezca la Oficina TIC.
- 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 para volver a intentar, o solicitar el desbloqueo a través de la Mesa de Servicios.
- La contraseña deberá cambiarse si se ha detectado anomalía en la cuenta de usuario.
- La contraseña no deberá ser visible en la pantalla, al momento de ser ingresada.
- No deberán ser reveladas a ninguna persona.
- Las contraseñas no se deberán 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 TIC.

A.9.4 Control de acceso a sistemas y aplicaciones

- Todo funcionario del MVCT, cualquiera sea su situación contractual, la dependencia a la cual pertenezca y el nivel de las tareas que desempeñe debe tener asociado un perfil de uso de los recursos de información, incluyendo el hardware y software asociado. La Oficina TIC debe mantener un directorio completo y actualizado de tales perfiles.
- La Oficina TIC debe establecer el método de autenticación de usuarios a adoptar por el Ministerio. El método que se escoja debe garantizar que el

repositorio de cuentas de usuario, perfiles y contraseñas para la autenticación de usuarios, se encuentre protegido de cualquier intento de acceso indebido o corrupción y cuente con logs de seguridad requeridos para las auditorias. Adicionalmente determinará cuales son los perfiles de usuarios que deben existir en el Ministerio y los atributos que debe tener cada uno de los diferentes perfiles para el control de accesos a los sistemas de información, bases de datos y servicios de información, donde se definan los niveles de acceso de los usuarios estándar del sistema comunes a cada categoría de puestos de trabajo y los administradores, asegurando que no comprometan la segregación de funciones; estos perfiles de usuarios deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

La Oficina TIC deberá definir los lineamientos para la restricción de acceso a la información teniendo en cuenta lo siguiente:

- Deberá 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.
- Deberá establecer el procedimiento y los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, deberá implementar para los desarrolladores internos o externos acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.
- Deberá 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.
- 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.
- 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.
- Los desarrolladores deberán asegurar que se inhabilitan las cuentas luego de un número establecido de intentos fallidos de ingreso a los sistemas desarrollados.
- 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.
- El uso de programas que puedan ser capaces de invalidar los controles del sistema y de la aplicación, deberán estar restringidos y estrictamente controlados.
- Las sesiones inactivas deberán cerrarse después de un período de inactividad definido y se deberán usar restricciones en los tiempos de conexión para

proporcionar una seguridad adicional a las aplicaciones misionales de alto riesgo.

- Toda la autenticación de aplicaciones o sistemas de información debe usar el método de autenticación definido por la Oficina TIC.
- La Oficina TIC debe elaborar, mantener y publicar los documentos de servicios de red que ofrece el Ministerio a sus funcionarios, contratistas y terceros.
- El acceso a aplicativos, sistemas de cómputo y los datos es responsabilidad exclusiva del funcionario propietario de los activos de información, según la matriz del inventario de activos de información.
- La Oficina TIC debe hacer mantenimiento continuo al directorio activo o al sistema empleado para la autenticación de usuarios con el objeto de desactivar las cuentas de usuarios que se desvincularon del Ministerio y verificar que las cuentas existentes corresponden a usuarios activos o vigentes en el Ministerio y su información está actualizada. Modificar los derechos de acceso de los usuarios que cambiaron de área y sus tareas. Cancelar cuentas de usuario redundantes. Inhabilitar cuentas que no hayan sido utilizadas por más de 90 días y estas no serán reactivadas hasta que la identidad del usuario haya sido verificada. Eliminar cuentas inactivas por más de 180 días. En el caso de existir excepciones, deberán ser debidamente justificadas y aprobadas.
- Las contraseñas de administrador de las aplicaciones o soluciones de software que producen, procesan, gestionan, o almacenan información de misión crítica del Ministerio, deben ser conservadas por la Alta Dirección y/o la Oficina TIC, estas deben ser cambiadas en intervalos regulares de tiempo, máximo de 360 días y/o en caso que el personal responsable de las mismas cambie de cargo o de dependencia. De igual manera las claves de administrador de servidores, equipos de comunicaciones y de seguridad deben ser conservadas por la Alta Dirección y la Oficina TIC, en el momento en que sea cambiada alguna de las contraseñas de estos equipos inmediatamente debe ser dada a conocer a estas dependencias.
- La Oficina TIC debe elaborar, mantener y actualizar el procedimiento y las guías para la correcta definición, uso y complejidad de contraseñas de usuario.

Los sistemas de información o aplicaciones deberán cumplir con:

- Después de cinco (5) minutos de inactividad del sistema, se considerará tiempo muerto y se deberá bloquear la sesión, sin cerrar las sesiones de aplicación o de red.
- No mostrar información del sistema, hasta que el proceso de inicio se haya completado.
- No suministrar mensajes de ayuda, durante el proceso de autenticación.
- Validar los datos de acceso, una vez que se han diligenciado todos los datos de entrada.
- Limitar el número de intentos fallidos de conexión auditando los intentos no exitosos hasta un máximo de tres (3) intentos.
- No mostrar las contraseñas digitadas con anterioridad.
- No transmitir la contraseña en texto claro.

- La Oficina TIC deberá 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 utilitarios que permitan escalar privilegios o evadir controles de seguridadinformáticos.
- La Oficina TIC deberá monitorear a los administradores de los recursos tecnológicos y serviciosde red, para que no hagan uso de utilitarios que permiten 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.
- La Oficina TIC deberá generar y mantener actualizado un listado de programas utilitarios privilegiados de la plataforma tecnológica, los servicios de red y sistemas de información.
- La Oficina TIC deberá retirar o deshabilitar los programas utilitarios privilegiados no autorizadosde la plataforma tecnológica, los servicios de red y sistemas de información.
- El acceso al código fuente del programa es limitado, solamente los ingenieros desarrolladoresy de soporte autorizados por la Oficina TIC o por los dueños de los activos de información pueden tener acceso.

A.10 CRIPTOGRAFÍA

A.10.1 Controles criptográficos

- Los responsables de la administración de la plataforma tecnológica deberán utilizar controles criptográficos en los siguientes casos:
  - Para la protección de claves de acceso a sistemas, datos y servicios.
- La Oficina TIC deberá disponer de mecanismos de cifrado en la transmisión de información clasificada o reservada.
- La Oficina TIC deberá disponer de herramientas que permitan el cifrado de medios de almacenamiento de información.
- Las áreas responsables o dueñas de los sistemas de información o aplicaciones deberán establecer controles criptográficos para la custodia de los usuarios administradores de cada una.

A.11 SEGURIDAD FÍSICA Y DEL ENTORNO

A.11.1 Áreas seguras

- El perímetro de las áreas que contienen la información y sus instalaciones de procesamientosensible o critico deberán estar protegidos de accesos no permitidos.
- Las puertas y ventanas de las áreas seguras deberán permanecer cerradas con llave cuandono hay supervisión o están desocupadas.
- Todos los puntos de acceso deberán tener un área de recepción con vigilancia u otro mediopara controlar el acceso físico al sitio o edificación.
- El perímetro de seguridad debe contar con vigilancia mediante CCTV y

debe ser monitoreado por el personal de vigilancia del MVCT.

- El Grupo de Recursos Físicos deberá señalizar las áreas de acceso restringido.
- El Grupo de Recursos Físicos deberá establecer un sistema de control de acceso a las instalaciones del MVCT, así como a las áreas demarcadas con acceso restringido dentro y fuera de las instalaciones principales del Ministerio.
- Las áreas de acceso restringido deben estar monitoreadas en su acceso por CCTV.
- El Grupo de Recursos Físicos y la Oficina TIC, serán los responsables de administrar el ingreso y salida del personal a los centros de cableado de las sedes del Ministerio.
    - El Grupo de Recursos Físicos y/o la Oficina TIC, autorizarán el ingreso a personal ajeno al MVCT a los centros de cableado para fines laborales, este deberá estar acompañado por quien sea autorizado, éste se hará responsable de la estadía del personal ajeno al MVCT durante el tiempo que permanezca en las instalaciones.
- Todo el personal que ingrese al centro de datos o a los centros de cableado deberá portar identificación visible y presentarla en la puerta de acceso antes de su ingreso y deberá diligenciar una bitácora en la cual se debe registrar la fecha y hora de su ingreso y salida, motivo de la visita, nombres, cédula, quien le autoriza el ingreso y/o si ingresa o retira elementos de estas áreas, y demás información que el Grupo de Recursos Físicos determine apropiadas.
- El Grupo de Recursos Físicos deberán controlar que los centros de cableado permanezcan siempre con las puertas de acceso cerradas y con controles de seguridad que mitiguen el acceso a personal no autorizado.
- El Grupo de Recursos Físicos deberá mantener en buen estado la infraestructura física de los centros de cableado, tales como puertas, cerraduras, ventanas, techos, paredes, pisos, aires acondicionados, cielos rasos, pisos falsos, entre otros.
- La Oficina TIC deberá 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 TIC y daños en infraestructura física (puertas, cerraduras, ventanas, techos, paredes, pisos, aires acondicionados, cielos rasos, pisos falsos, entre otros) al Grupo de Recursos Físicos.
- El Grupo de Recursos Físicos y la Oficina TIC, son los responsables del cumplimiento del protocolo de aseo en los centros de cableado.
- El Grupo de Recursos Físicos será responsable de la identificación y señalización necesaria de los centros de cableado.
- El Grupo de Recursos Físicos deberá implementar y administrar los circuitos cerrados de televisión (CCTV) para los centros de cableado.
- El Grupo de Recursos Físicos deberá respaldar los videos generados por las cámaras de vigilancia no menor a 60 días.
- El Grupo de Recursos Físicos, deberá mantener libre de objetos o elementos que no sean propios en la operación en el centro de datos.

- El Grupo de Recursos Físicos deberá controlar y monitorear a través de CCTV el ingreso a las áreas seguras.
- El Grupo de Recursos Físicos deberá establecer circuito cerrado de televisión (CCTV), que cubra el acceso al área y al funcionario que utilice los equipos financieros de pago.
- El Grupo de Recursos Físicos y la Oficina TIC, deberán implementar controles que permitan hacer seguimiento a variables de humedad y temperatura a los centros de cableado.
- El Grupo de Recursos Físicos deberá realizar revisiones periódicas de las oficinas que estén vacías asegurando que estén cerradas con llave.
- El Grupo de Recursos Físicos deberá restringir al interior del Ministerio el uso de equipos fotográficos, 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.
- 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.
- El Grupo de Recursos Físicos deberá establecer lineamientos para los controles de área de despacho y carga teniendo en cuenta lo siguiente:
  - El material que ingresa se deberá inspeccionar y examinar para determinar la presencia de materiales peligrosos.

A.11.2 Equipos

El Grupo de Recursos Físicos deberá establecer lineamientos para los controles de ubicación y protección de los equipos teniendo en cuenta lo siguiente:

- Los equipos de cómputo e impresoras deberán estar situados y protegidos para reducir el riesgo contra amenazas ambientales y de acceso no autorizado.
- Todos los equipos portátiles deben estar protegidos por guaya de seguridad.
- Establecer directrices acerca de comer, consumir líquidos y fumar en cercanías de las instalaciones de procesamiento de información.

- La Oficina de Control Interno podrá auditar los registros resultado de las auditorias efectuadas por la segunda línea de defensa correspondientes al acceso a las áreas protegidas, en el marco de desarrollo del plan anual de auditoria como tercera línea de defensa.

- El Ministerio debe implementar el uso de un control de acceso biométrico u otro control a las áreas restringidas para evitar la presencia de desconocidos no escoltados por personal autorizado.

- La Oficina TIC establece que para el uso de la red de energía regulada en los puestos de trabajo solo se deberán conectar equipos como computadores de escritorio, portátiles y pantallas; los otros elementos deberán conectarse a la red eléctrica no regulada.

- El Grupo de Recursos Físicos con el apoyo de la Oficina TIC deberán 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.
- El Grupo de Recursos Físicos deberá suministrar plantas eléctricas y UPS a las sedes del MVCT y garantizar su manteamiento preventivo y correctivo.
- El cableado que transporta datos y de suministro de energía deberán estar protegidos contra la interceptación, interferencia o daños.
- Los cables de energía eléctrica deberán estar separados de los cables de comunicaciones para evitar interferencia.
- Deberán tener en cuenta las consideraciones técnicas de las normas vigentes y el reglamento técnico de instalaciones eléctricas RETIE.
- 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.
- La Oficina TIC deberá definir mecanismos de soporte y mantenimiento a los equipos.
- Las actividades de mantenimiento tanto preventivo como correctivo deberán registrarse.
- Solo el personal autorizado deberá llevar a cabo el mantenimiento o las reparaciones a los equipos tecnológicos del MVCT.
- En caso de presentarse una falla o problema de hardware o software en una estación de trabajo o equipo portátil de propiedad del MVCT, el usuario responsable del mismo deberá informarlo a la Oficina TIC, para una asistencia especializada, y por ningún motivo deberá intentar resolver el problema.
- Las actividades de mantenimiento de los servidores, elementos de comunicaciones, energía o cualquiera que pueda ocasionar una suspensión en el servicio, deberán ser programadas.
- Los equipos que requieran salir de las instalaciones del MVCT para reparación o mantenimiento deberán estar debidamente autorizados.
- El Grupo de Recursos Físicos deberá registrar cuando los equipos de cómputo ingresan y se retiran de las instalaciones del MVCT.
- El Grupo de Recursos Físicos deberá llevar un control en el almacén de los equipos cuando se asignan y cuando se hace su devolución.
- Todo equipo de cómputo que se quiera retirar de las instalaciones del MVCT, deberá ser autorizado por el Jefe inmediato e informado a Seguridad Física para que se permita su salida.
- El ingreso y salida de servidores y de dispositivos de comunicaciones de las instalaciones del MVCT debe estar debidamente autorizado por el Grupo de Recursos Físicos.
- La Oficina TIC deberá garantizar que cuando un dispositivo vaya a ser reasignado, este deberá ser formateado e instalado la línea base de software.
- La Oficina TIC deberá garantizar que cuando un dispositivo vaya a ser

retirado de servicio, deberá realizarse la eliminación de toda información mediante borrado seguro teniendo en cuenta que previo a esta actividad deberá realizar copia de seguridad de la misma.

- Los Colaboradores del MVCT, 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.
- Los Colaboradores del MVCT, deberán 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 computador y cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.
- Los Colaboradores del MVCT que impriman documentos con clasificación (Clasificada – Reservada), estos deberán ser retirados de la impresora inmediatamente y no se deberán dejar en el escritorio sin custodia.
- No se deberá reutilizar documentos impresos con clasificación (Clasificada – Reservada), estos deberán ser destruidos y no deberán estar como papel reciclable.
- Los documentos impresos con clasificación (Clasificada – Reservada), no deberán publicarse.
- Los lugares de trabajo de los Colaboradores del MVCT y terceras partes que prestan sus servicios al Ministerio y cuyas funciones no obliguen a la atención directa de ciudadanos deberán localizarse preferiblemente en ubicaciones físicas que no queden expuestas al público para minimizar los riesgos asociados al acceso no autorizado de la información o a los equipos informáticos.
- Todos los computadores del MVCT deberán tener configurado y en operación un protector de pantalla con tiempo máximo de cinco (5) minutos para que se active cuando el equipo no esté en uso.
- Los equipos críticos de comunicaciones deben ser alimentados por sistemas de potencia eléctrica regulados y estar protegidos por UPS.
- La Oficina TIC debe asegurar que la infraestructura de servicios de TI esté cubierta por mantenimiento y soporte adecuados de hardware y software.
- Los funcionarios y contratistas, que tengan acceso a los equipos que componen la infraestructura tecnológica del MVCT no pueden fumar, beber o consumir algún tipo de alimento cerca de los equipos.
- Las estaciones de trabajo, equipos portátiles y demás recursos informáticos como impresoras, fotocopiadoras, máquinas de fax y video proyectores, entre otros, de propiedad del MVCT no deben ser utilizados para actividades personales o ajenas al Ministerio.
- Las estaciones de trabajo, equipos portátiles y demás recursos informáticos del MVCT deben ser operados solamente por personal autorizado y/o el responsable de los mismos.
- La protección física de las estaciones de trabajo, equipos portátiles y demás recursos informáticos corresponde a los responsables o custodios de los

mismos y es su deber, notificar cualquier eventualidad que ocurra sobre dichos equipos a la Oficina TIC.

- Los equipos que hacen parte de la infraestructura tecnológica del MVCT tales como, servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, subestaciones eléctricas, aires acondicionados, así como estaciones de trabajo y dispositivos de almacenamiento (digitales o no digitales), copias de respaldo, y/o comunicación móvil que contengan y/o brinden servicios de soporte a la información crítica de las dependencias, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos. De igual manera, se deben adoptar los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de peligros ambientales y amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.
- Cuando un funcionario inicie o termine su vinculación laboral con el MVCT, sea trasladado entre áreas, sedes, o por alguna otra circunstancia deje de utilizar el recurso informático suministrado con carácter permanente, deberá entregar dicho recurso formalmente a la Oficina TIC o, en su defecto, a su Jefe inmediato.
- El alistamiento de las estaciones de trabajo y equipos portátiles es responsabilidad de la Oficina TIC, así como la eliminación segura de la información de los mismos.
- La Oficina TIC, debe procurar que todos los recursos informáticos tales como servidores, dispositivos de comunicación, estaciones de trabajo, equipos portátiles e impresoras, entre otros, que sean propiedad del MVCT se encuentren continuamente actualizados en aras de conservar e incrementar la calidad del servicio que prestan, mediante la mejora de su desempeño y obtener mayor estabilidad y protección ante amenazas.
- La Oficina TIC será 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.
- La Oficina TIC será responsable de mantener organizado e identificado el cableado en los racks de los centros cableado.

A.12 SEGURIDAD DE LAS OPERACIONES

A.12.1 Procedimientos operacionales y responsabilidades

- ☐ La Oficina TIC deberá documentar y mantener actualizados todos sus procedimientos operativos para garantizar la disponibilidad, integridad y confidencialidad de la información.
- ☐ La Oficina TIC deberá poner a disposición de todos los colaboradores los procedimientos de operación.
- ☐ La configuración de servidores, equipos activos, enrutadores, switches, firewall, sistemas de detección y protección de intrusos y otros dispositivos de seguridad de red; debe ser documentada para cada equipo o dispositivo,

respaldada por copia de seguridad y mantenida por la Oficina TIC.

- ☐ Toda modificación en la configuración de los servidores, equipos activos y demás equipos de red debe ser documentada y junto con el respaldo de la nueva configuración inmediatamente actualizada a los responsables de conservar dicha información.
- ☐ Todo equipo de TI debe ser revisado, registrado y aprobado por la Oficina TIC antes de conectarse a cualquier nodo de la red de comunicaciones y datos del Ministerio. Dicha oficina debe desconectar aquellos dispositivos que no estén aprobados y reportar tal conexión como un incidente de seguridad.
- ☐ La Oficina TIC 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 los responsables y tareas en la gestión de cambios.
- ☐ La Oficina TIC debe establecer un comité de cambios, quien se encargará de evaluar, aprobar o negar la implementación de los cambios.
- ☐ La Oficina TIC deberá documentar la gestión de capacidad la cual le 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 MVCT.
  - Documentar los acuerdos de niveles de servicio.
  - Asignar los recursos adecuados de hardware y software, para todos los servicios y aplicaciones de tecnología.
  - Realizar las recomendaciones de mejora de la infraestructura de tecnología.
  - Definir los indicadores de rendimiento correspondientes a la gestión de capacidad.
  - Deberá asignar un responsable de la gestión de capacidad.
- ☐ La Oficina TIC deberá establecer cuotas de almacenamiento para cada recurso compartido, adicional a esto se deberá definir umbrales que permitan notificar al administrador del servicio de almacenamiento y al administrador de carpeta que el espacio asignado ya está llegando a su límite. Cada cuota está sujeta a las necesidades de cada área y a la proyección de crecimiento de cada una de ellas.
- ☐ La Oficina TIC deberá restringir excepto en las dependencias que por el desarrollo de sus funciones sean necesarios almacenamiento de tipo de archivos como:
  - Audio (.avi, .mpeg, .mp3, .mid o. midi, wav, wma, cda, ogg, ogm, .aac, .ac3, flac, mp4, aym)
  - Video (.avi,.mpeg, .mov, .wmv, .rm, .flv)
  - Archivos ejecutables (.exe, .bat, .com, bin)
  - Archivos de páginas web (html, xml, jsp, asp)
  - Archivos de sistema (.acm,.dll,.ocx,.sys,.vxd)

- ☐ La Oficina TIC deberá crear grupos de seguridad en el directorio activo con rol de lectura y escritura, de acuerdo con las necesidades solicitadas por cada dependencia. Se deberá configurar los grupos de seguridad en cada una de las carpetas de primer nivel.
- ☐ La Oficina TIC deberá generar reportes en cada una de sus soluciones, evidenciando que tipos de archivos se encuentran alojados, archivos por propietarios, archivos duplicados, archivos grandes, archivos no usados recientemente, para determinar acciones que eviten posibles fallas en la solución de almacenamiento del MVCT.
- ☐ La Oficina TIC deberá realizar la separación de ambientes de desarrollo, pruebas y producción, los cuales deberán estar separados de manera física y lógica.
- ☐ La Oficina TIC deberá definir y documentar los lineamientos a seguir para la transferencia entre ambientes.
- ☐ La Oficina TIC deberá utilizar datos que no sean sensibles para el MVCT, en los ambientes de prueba y desarrollo.
- ☐ La Oficina TIC deberá 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.
- ☐ La Oficina TIC deberá garantizar que los desarrolladores realicen su trabajo exclusivamente en el ambiente de desarrollo y nunca en los ambientes de pruebas o producción.

A.12.2 Protección contra códigos maliciosos

- ☐ El MVCT debe contar con las herramientas de seguridad tales como antivirus, antiSpam, antispyware, seguridad perimetral y otras aplicaciones que permitan brindar la adecuada protección contra código malicioso, malware, phishing, ransomware, entre otros, con el fin de evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso.
- ☐ La Oficina TIC deberá realizar campañas de concienciación a usuarios en materia de protección, prevención y recuperación contra códigos maliciosos.
- ☐ La Oficina TIC deberá dictar los lineamientos para la instalación de software antivirus que brinde protección contra códigos maliciosos en todos los recursos informáticos del MVCT y asegurar que estas herramientas no puedan ser deshabilitadas, así como mantenerlas actualizadas permanentemente.
- ☐ La Oficina TIC deberá realizar la actualización continua de la base de firmas y parches correspondiente del software de antivirus y actualizaciones de sistema operativo.
- ☐ Todo mensaje sospechoso de procedencia desconocida deberá ser inmediatamente reportado a la Oficina TIC a través de la mesa de servicios, tomando las medidas de control necesarias.
- ☐ Los funcionarios y/o contratistas que detecten alguna infección por software malicioso deben reportar a la Oficina TIC, mediante la mesa de servicio.

- ☐ Los funcionarios y/o contratistas tendrán prohibido, la desinstalación y/o desactivación de software y herramientas de seguridad aprobadas por la Oficina TIC.
- ☐ Los funcionarios y/o contratistas tienen prohibido, escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica del Ministerio.

A.12.3 Copias de respaldo

- El MVCT debe asegurar que la información con cierto nivel de clasificación, definida en conjunto por la Oficina TIC y las dependencias responsables de la misma, contenida en la plataforma tecnológica del Ministerio, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sean periódicamente respaldadas mediante mecanismos y controles que garanticen su identificación, protección, integridad y disponibilidad. Adicionalmente, se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado.
- La Oficina TIC establecerá procedimientos o un plan de copia de seguridad del MVCT donde se establezca esquemas de qué, cuándo, con qué periodicidad, cual es la criticidad explícitos de respaldo, número de copias y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia, identificación y definirá conjuntamente con las dependencias los períodos de retención de la misma. Adicionalmente, debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información respaldada.
- La Oficina TIC deberá realizar y mantener copias de seguridad de la información digital solicitadas por el Líder funcional o Líder técnico.
- La Oficina TIC deberá definir la custodia y almacenamiento de las copias.
- La Oficina TIC deberá tener un inventario y bitácora de las copias que se realizan y de las copias que se restauran.
- La Oficina TIC deberá dar los lineamientos para la realización de las copias de seguridad de:
    - Bases de datos en producción.
    - Software de aplicaciones.
    - Sistemas operativos.
    - Software base del MVCT.

- Cuentas de correo electrónico con valor estratégico para el MVCT (Ministro, Viceministros, Jefes, Directores, Subdirectores, Asesores, Administradores de Sistemas, entre otros).

- La Oficina TIC deberá generar mecanismos que mantengan la integridad y confidencialidad delas copias de seguridad.
- Los colaboradores son responsables de la información que resida en el computador asignado y serán los encargados de mantener copia de sus archivos más sensibles entregando al supervisor del contrato o jefe inmediato en custodia al finalizar la vinculación. En caso de que los colaboradores requieran la ejecución de un respaldo de información, lo pueden solicitar a la Oficina TIC a través de la mesa de servicios.
- Las copias de seguridad de la información (back-up), deberán ser almacenadas dentro y fuera del Ministerio, como medida preventiva para asegurar la recuperación total de los datos. En casode tener una sola copia debe ser llevada fuera de la sede o sitio del procesamiento de datos. Eltraslado de los medios y/o dispositivos debe ser realizado por personal debidamente autorizado,teniendo en cuentas las medidas de seguridad.
- Los medios magnéticos con al menos una de las copias que contienen la información crítica, deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguardan dichas copias, debe tener los controles de seguridad adecuados, cumplir con máximas medidas de protección y seguridad física apropiados.

A.12.4 Registro y seguimiento

- La Oficina TIC deberá realizar monitoreo periódico sobre los aplicativos y velar por la generaciónde los registros de auditoría (log´s).
- La Oficina TIC deberá generar registros de auditoría que contengan excepciones o eventos relacionados a la seguridad en los sistemas de información que se consideren.
- La Oficina TIC deberá salvaguardar los registros de auditoría que se generen de cada sistema.
- La Oficina TIC deberá monitorear excepciones o los eventos de la seguridad de información.
- La Oficina TIC deberá monitorear la infraestructura tecnológica para garantizar que estos seanusados para la misionalidad de la entidad.
- La Oficina TIC o el proveedor de tecnología deberá 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.

A.12.5 Control de software operacional

- La Oficina deberá controlar y tener registros de la actualización del software en producción, aplicaciones y librerías de programas propios del MVCT.
- La Oficina TIC deberá usar controles para proteger todo el software implementado y ladocumentación del sistema.
- La Oficina TIC deberá conservar las versiones anteriores del software de aplicación como una medida de contingencia, junto con toda la información y

parámetros, procedimientos, detalles de configuración y software de soporte anteriores.

- Las actualizaciones del software, de las aplicaciones y librerías las deben realizar únicamente colaboradores que tengan los roles, privilegios y el conocimiento en cada una de las aplicaciones.
- Los servidores de aplicación únicamente deben alojar los códigos ejecutables aprobados de las mismas, de ninguna manera se debe alojar el código fuente o de desarrollo ni los compiladores.
- La Oficina TIC deberá establecer estrategias de retroceso (rollback) antes de implementar los cambios.

A.12.6 Gestión de la vulnerabilidad técnica

La Oficina TIC deberá:

- Realizar de manera periódica revisión de vulnerabilidades técnicas por medio de pruebas de penetración, a los sistemas de información críticos y misionales.
- Documentar, informar, gestionar y corregir, los hallazgos de las vulnerabilidades adoptando las acciones preventivas y correctivas necesarias para minimizar el nivel de riesgo y reducir el impacto.
- 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.
- Si está disponible una actualización de una fuente legítima, se deberán valorar los riesgos asociados con la instalación de la actualización y se deberán probar y evaluar antes de su instalación, para asegurarse de que son eficaces y no producen efectos secundarios que no se puedan tolerar.
- Todas las instalaciones de software que se realicen sobre equipos del Ministerio deben ser aprobadas por la Oficina TIC, de acuerdo con los procedimientos elaborados para tal fin.
- No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor, en especial la Ley 23 de 1982 y relacionadas. La Oficina TIC debe desinstalar cualquier software ilegal y registrar este hecho como un incidente de seguridad.
- Corresponde a la Oficina TIC mantener una base de datos actualizada que contenga un inventario del software autorizado para su uso e instalación en los servidores, estaciones de trabajo y demás equipos del Ministerio.
- La Oficina TIC deberá 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 derechos de autor.
- La Oficina TIC podrá en cualquier momento realizar una inspección del software instalado en los equipos de cómputo.

Sólo está permitido el uso de software licenciado por el MVCT y/o aquel que sin requerir licencia de uso comercial sea expresamente autorizado por la Oficina TIC. Las

aplicaciones desarrolladas al interior del MVCT, en desarrollo de su misión, deberán ser reportadas a la Oficina TIC, para su administración.

- La Oficina TIC es la única dependencia autorizada para la administración del software, el cual no deberá ser copiado, suministrado a terceros o utilizado para fines personales.

A.12.7 Consideraciones sobre auditorías de sistemas de información

- La Oficina TIC, como segunda línea y líder de la política de seguridad digital, planificará 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.
- La Oficina TIC, como segunda línea y líder de la política de seguridad digital, deberá mantener los documentos, dispositivos y medios utilizados para las auditorias de los sistemas de información custodiados de accesos no autorizados.
- La Oficina de Control Interno realizará evaluaciones independientes basadas en las muestras de los sistemas de información y al SGSI del MVCT, con un enfoque en riesgos de seguridad digital, de acuerdo a lo establecido en su Plan Anual de Auditorías y a la disponibilidad de los recursos necesarios para su ejecución conforme a las necesidades y expectativas de la Alta Dirección, teniendo en cuenta los resultados de las auditorías realizadas por la segunda línea de defensa.

A.13 SEGURIDAD DE LAS COMUNICACIONES

A.13.1 Gestión de la seguridad de las redes

- La plataforma tecnológica del MVCT que soporta los sistemas de Información 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 si así se requiere. La Oficina TIC es la encargada de establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.
- La Oficina TIC deberá realizar segmentación de redes para colaboradores y visitantes del MVCT.
- La Oficina TIC deberá establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.
- La Oficina TIC es la responsable de mantener disponible toda la infraestructura de red que soportan los servicios tecnológicos del

Ministerio.

- La Oficina TIC debe establecer los procedimientos, guías y demás documentación que permitala gestión de los dispositivos de red del Ministerio.
- La Oficina TIC deberá disponer de una zona desmilitarizada o DMZ, entre la red interna delMVCT y la red externa (internet) con el objetivo delimitar conexiones desde la red interna hacia nternet y limitar las conexiones desde internet hacia la red interna del MVCT con los siguientescriterios:
    - EL tráfico de la red externa a la DMZ está limitado.
    - El tráfico de la red externa a la red interna deberá estar restringido y monitoreado.
    - El tráfico de la red interna a la DMZ está limitado.
    - El tráfico de la red interna a la red externa está limitado
- La DMZ deberá implementar controles para ofrecer servicios que se necesitan desde internet. Estos servicios deberán ser monitoreados con el fin de prevenir ataques.
- La arquitectura de la DMZ deberá estar aislada de la red interna del MVCT de forma que no permita el acceso no autorizado a la red interna, por lo que se deberán diseñar redes perimetrales con los siguientes objetivos:
    - No se pueden hacer consultas directas a la red interna del MVCT desde redes externas e internet.
    - Se deberá realizar la segmentación de redes y listas de acceso a los servicios del MVCT, tales como servidores, administración, invitados, entre otros.
    - El acceso a la red de datos del MVCT y a los sistemas de información soportados por la misma, es de carácter restringido. Se concederán permisos con base a "la necesidad de conocer" y el "acceso mínimo requerido".
    - La conexión a la red wifi institucional para funcionarios deberá ser administrada desde la Oficina TIC mediante un SSID (Service Set Identifier) único a nivel de las sedes del Ministerio, la autenticación deberá ser con usuario y contraseña de directorio activo.
    - La conexión a la red institucional para visitantes deberá tener un SSID y contraseñas diferentes para cada sede administrativa (Sede botica, fragua, calle 18 y demás), administrada por la Oficina TIC; la contraseña deberá cambiar periódicamente y solo estará disponible en el horario laboral definido en la resolución de horario de cada sede.
    - No se podrá conectar dispositivos celulares personales a la red wifi de funcionarios, salvo los del despacho del Ministro y sus Viceministros y los aprobados por la Oficina TIC a travésde una solicitud en la herramienta de mesa de servicios.
- Los colaboradores que requieran acceder a algunos recursos informáticos del MVCT fuera delas instalaciones de la Entidad deberán realizarlo a través de una conexión de red virtual privada (VPN), previa autorización del Jefe inmediato o Supervisor de contrato y del Jefe de laOficina TIC
- Es responsabilidad de los administradores de recursos tecnológicos

garantizar que los puertosfísicos y lógicos de diagnóstico y configuración de plataformas que soporten sistemas de información, deban estar siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.

A.13.2 Transferencia de información

- La Oficina TIC deberá definir controles para la transferencia de información a través de redespúblicas para las aplicaciones del MVCT.
- La Oficina TIC deberá establecer procedimientos para la detección de software malicioso yprotección contra éste.
- La Oficina TIC deberá establecer controles para proteger la información que se transmite comodocumentos adjuntos a través del correo electrónico del MVCT.
- La Oficina TIC deberá contar con los lineamientos para proteger la información transferida con respecto a la interceptación, copiado, modificación, enrutado y destrucción de la misma.
- El intercambio de información digital pública clasificada y pública reservada, debe realizarse por canales cifrados que garanticen la protección de la confidencialidad de la información y quecumpla con la política de controles criptográficos, esto debe quedar registrado en los convenioso acuerdos de intercambio de información que firmen las partes.
- El Grupo de Atención al Usuario y Archivo dictará directrices sobre retención, disposición y transferencia de la información del MVCT, de acuerdo con la legislación y reglamentaciones locales y nacionales.
- La Oficina TIC y la Oficina Asesora Jurídica deberán establecer un acuerdo para la transferencia de información entre el MVCT y las partes externas.
- Todo intercambio de información electrónica perteneciente al MVCT con terceros, debe ser respaldado con un acuerdo (convenio o contrato), incluyendo una cláusula de confidencialidad y no divulgación de la información proporcionada.
- Para el transporte de medios físicos que contengan información digital o electrónica del Ministerio, se debe generar un registro de entrega de estos medios y recepción de estos y se debe transportar en un dispositivo con un sello de seguridad que garantice que en su desplazamiento no ha sido intervenido por un tercero.
- Para la apertura de ese sello se debe generar un registro y garantizar que no se reutilice el sello.
- Se deben transportar estos medios en un recipiente que proteja al activo de amenazas ambientales.
- Toda información enviada desde el MVCT a través de correos electrónicos deberá incluir en supie de página la siguiente advertencia:

  "Este mensaje y cualquier archivo que se adjunte al mismo es confidencial y podría contener información clasificada y reservada del MVCT, para el uso exclusivo de su destinatario. Si ustedno es el receptor autorizado, cualquier retención, difusión, distribución o copia de este mensaje es prohibida y

sancionada por la ley. Si por error recibe este mensaje, por favor reenviarlo al remitente y borrar el mensaje recibido inmediatamente".

- Solo se puede realizar intercambio de información del MVCT entre su personal cuando dicho intercambio corresponda a actividades relacionadas con el desarrollo de sus actividades.
- Se deberán identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
- Como parte de sus términos y condiciones iniciales de trabajo, los colaboradores, cualquiera sea su nivel jerárquico dentro del MVCT, firmarán un compromiso de confidencialidad o no divulgación, en lo que respecta al tratamiento de la información del MVCT.
- En el caso de que sea personal externo que ejecute tareas propias del MVCT y haya sido contratado en el marco de un contrato o convenio con el MVCT, deberá reposar en la carpeta de ejecución del contrato un compromiso de confidencialidad firmado entre el MVCT (Supervisor del Contrato) y el Representante Legal.
- Para el caso de contratistas y proveedores, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos del MVCT a personas o entidades externas.
- Todo funcionario del MVCT es responsable de proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.
- Los propietarios de la información que se requiere intercambiar son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de la misma y los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad, disponibilidad y requeridos.
- Los acuerdos de confidencialidad deben aceptarse por los contratistas y proveedores como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

A.14.1 Requisitos de seguridad de los sistemas de información

La Oficina TIC deberá cumplir con los siguientes lineamientos de seguridad:

☐ La Oficina TIC debe elegir, elaborar, mantener y difundir un documento que describa las "Características y metodología para el desarrollo y adquisición de sistemas de información en el MVCT", debe especificar los requisitos de seguridad y el framework que debe utilizar, para contratar la adquisición,

desarrollo o mejoras de sus sistemas de información o soluciones de software, los cuales debe cumplir el contratista o casa de software para el suministro de la solución. El documento debe incluir un conjunto estandarizado de requerimientos de seguridad, conceptos, buenas prácticas, criterios, procesos, plantillas y demás características que sirvan para adquirir o contratar los desarrollos de las soluciones de software en un ambiente de mitigación del riesgo y aseguramiento de la calidad.

- ☐ Todo proyecto de adquisición o compra de software debe contar con un documento de identificación y valoración de riesgos del proyecto aprobado por la Oficina de TIC. El Ministerio no debe emprender procesos de adquisición, desarrollo o mantenimiento de aplicativos o soluciones de software que tengan asociados riesgos altos no mitigados.
- ☐ Los aplicativos o soluciones de software adquiridos a través de terceras partes deben certificar por escrito el cumplimiento de los requisitos y estándares de calidad en el proceso de desarrollo. El desarrollo de software, deberá incluir los siguientes puntos:
  - Acuerdos de licencias, propiedad del código fuente y derechos conferidos.
  - Requerimientos con respecto a la calidad del código fuente y la existencia de garantías.
  - Procedimientos de certificación y verificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos en los términos de referencia.
  - Acuerdos de custodia de las fuentes del software (y cualquier otra información requerida) en caso de quiebra de la tercera parte.

- En caso de desarrollos propios al interior del Ministerio, estos se deben separar en ambientes de desarrollo, prueba y producción, en diferentes procesadores y dominios.
- Todo sistema de información y/o aplicación que se vaya a desarrollar debe estar integrado al directorio activo como fuente de autenticación al mismo.
- La Oficina TIC debe asegurar que:
  - En el desarrollo o adquisición de sistemas de información se definan todos los requerimientos necesarios para su buen funcionamiento.
  - Exista integración de los sistemas de información con los que cuenta la organización.
  - Se ejecuten todas las pruebas necesarias antes de la puesta en funcionamiento (producción) a cualquier solución que se implemente.
  - Se documenten los sistemas de información y/o aplicaciones y que se realicen las actualizaciones correspondientes cuando estas son modificadas. Toda adquisición, desarrollo o modificación de sistemas de información y/o aplicación deberán incluir el suministro y/o actualización de la documentación correspondiente del sistema o módulo:
    - Especificaciones funcionales.
    - Especificaciones de seguridad.

    - Manual de Instalación y configuración.
    - Manual de administración, operación y mantenimiento.
    - Manual de usuario.
  - Sean actualizados los documentos de inventario de sistemas de información en la OficinaTIC, con las modificaciones y adquisiciones que se generen.
  - La seguridad de la información sea parte integral en el ciclo de vida de las aplicaciones.
  - Se entreguen los medios (programa fuente, programas objeto, licencias y manuales), de los sistemas de información para ser inventariados, contar con las garantías y licenciamientos como resultado de la adquisición o desarrollo realizado.
- Se deberán realizar pruebas de funcionamiento y de seguridad a los nuevos sistemas, actualizaciones y/o aplicaciones en ambiente de pruebas, para validar la necesidad y operatividad de estos, previo a la aprobación e implementación.
- Cualquier otra copia del programa original será considerada como una copia no autorizada y su utilización conlleva a las sanciones administrativas y legales pertinentes.
- La Oficina TIC será la única dependencia autorizada para realizar copia de seguridad del software original.
- El software proporcionado por la Oficina TIC no puede ser copiado o suministrado a terceros.
- Cualquier desarrollo deberá implementar métodos y/o técnicas para el desarrollo de software seguro, estas deben incluir definiciones y requerimientos de seguridad, buenas prácticas para desarrollo, que le permita a los desarrolladores aplicarlas de manera clara y eficiente.
- Toda aplicación o sistema de información que deba exponerse en internet debe contar con uncertificado digital valido.
- La Oficina TIC deberá definir controles para la transferencia de información a través de redes públicas para las aplicaciones del MVCT.
- La Oficina TIC deberá disponer de controles para realizar transferencias completas, sin alteraciones y visualizaciones no autorizadas de la información entre las aplicaciones del MVCT, teniendo en cuenta los siguientes criterios
  - 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.

- 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 falladurante el proceso de autenticación y en su lugar, se deben generar mensajes generales de falla. Los desarrolladores deberán asegurar que no se despliegan en la pantalla las contraseñasingresadas, así como deberán deshabilitar la funcionalidad de

recordar campos de contraseña.

- Los desarrolladores deberán asegurar que se inhabilitan las cuentas luego de un número establecido de intentos fallidos de ingreso a los sistemas desarrollados.
- 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.
- Toda aplicación debe controlar el tiempo de inactividad en las sesiones, las cuales deberán cerrarse después de un período de inactividad definido máximo 5 minutos y se deberán usar restricciones en los tiempos de conexión para proporcionar una seguridad adicional a las aplicaciones misionales de alto riesgo.

A.14. 2 Seguridad en los procesos de desarrollo y de soporte

☐ La Oficina TIC cuando realice o contrate desarrollos de aplicaciones o sistemas de información deberá tener en cuenta como mínimo 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 encontrar y resolver vulnerabilidades.
- Reutilización de código.
- Mantener un rastro de auditoria de los cambios.

☐ Cuando la Oficina TIC desarrolle o realice mejora a las aplicaciones o sistemas e información deberán definir controles para que los cambios realizados sean documentados, teniendo en cuenta la integridad de los sistemas y/o aplicaciones desde las primeras etapas de diseño y a través de los mantenimientos posteriores.

☐ La Oficina TIC deberá definir un proceso formal para inclusión y cambios importantes de los sistemas de información y/o aplicaciones involucrando pruebas, control de calidad e implementación cuando se realicen actualizaciones o nuevos desarrollos.

☐ La Oficina TIC deberá guardar en un repositorio, las versiones anteriores de cada sistema de información que es actualizado.

☐ Todo cambio a nivel de aplicación y/o sistema de información debe notificarse con tiempo al dueño del activo permitiendo realizar pruebas y revisiones apropiadas antes de su implementación.

☐ Todo cambio que se realice a un sistema de información o a una aplicación siempre debe hacerse en un ambiente de desarrollo nunca sobre el ambiente de producción.

☐ Todos los colaboradores del ministerio deberán evitar realizar 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 MVCT.
- La compatibilidad con otro software en uso.

☐ La Oficina TIC deberá conservar el software original cuando se hayan realizado cambios en los paquetes del mismo.

☐ La Oficina TIC deberá 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 MVCT.
- 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.

☐ La Oficina TIC deberá 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.

☐ La Oficina TIC deberá contemplar en los cambios y en los nuevos sistemas de información, pruebas asociadas a seguridad de la información.

☐ La Oficina TIC deberá contar en sus pruebas de aceptación la verificación de los requisitos de seguridad de la información.

☐ Para los sistemas adquiridos o desarrollos contratados con terceros, el proveedor debe entregar resultados de pruebas de vulnerabilidad, los cuales

no deben tener vulnerabilidades críticas ni altas ni medias. Para los desarrollos internos se deben realizar pruebas de vulnerabilidad y se debe recibir a producción si no hay vulnerabilidades críticas ni altas ni medias.

- ☐ La Oficina TIC deberá definir controles para que los cambios en los sistemas de información en el MVCT sean documentados, teniendo en cuenta la integridad de los sistemas desde las primeras etapas de diseño y a través de los mantenimientos posteriores.

A.14.3 Datos de prueba

- ☐ En la fase de pruebas de los sistemas de información desarrollados o adquiridos, se deben utilizar datos despersonalizados (es decir, no datos de producción).
- ☐ Si se utilizan datos de producción, estos deben ser entregados a un funcionario responsable delos mismos, quien debe firmar el compromiso de confidencialidad y no divulgación de la información sobre los datos recibidos para pruebas. Una vez terminadas las pruebas estos deben ser borrados de manera segura.
- ☐ En cumplimiento de los requisitos legales de privacidad y seguridad de la información, los datos de prueba no deben contener información que permitan la identificación de la persona natural ojurídica a la que pertenezca la información.
- ☐ La Oficina TIC deberá evitar durante la ejecución de pruebas en ambientes de desarrollo el uso de datos que contengan información personal o información sensible del MVCT que este contenida en el ambiente de producción de las aplicaciones.
- ☐ La Oficina TIC deberá tener en cuenta controles de acceso a los ambientes de producción y deprueba.

A.15 RELACIONES CON LOS PROVEEDORES

A.15.1 Seguridad de la información en las relaciones con los proveedores

- Todas las dependencias deberán establecer lineamientos para el cumplimiento de las obligaciones contractuales del SGSI con terceros o proveedores.
- Todas las dependencias deberán establecer en el momento de suscribirse contratos de apoyo a la gestión que se desarrollen dentro del MVCT, los riesgos asociados a la seguridad de la información, los compromisos establecidos de confidencialidad de la información y el cumplimiento de las políticas de seguridad de la información del MVCT.
- Todas las dependencias deberán establecer en los contratos con terceros y proveedores los requisitos legales y regulatorios relacionados con la protección de datos personales, los derechos de propiedad intelectual y derechos de autor.
- La Oficina TIC deberá 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.

- Cada dependencia del Ministerio que establezca relación con proveedores y su cadena de suministro, solicitará capacitación periódica a la Oficina TIC referente a seguridad de la información con el fin de dar a conocer las políticas que tiene el Ministerio.
- Todos los proveedores, usuarios externos y funcionarios de entidades externas deben estar autorizados por un funcionario del Ministerio quien será responsable del control y vigilancia del uso adecuado de la información y los recursos de TI institucionales.

A.15.2 Gestión de la prestación de servicios de proveedores

- La Oficina TIC deberá documentar, establecer controles y permisos cuando un tercero o proveedor requiera tener accesos a la información por medio de la infraestructura tecnológica del MVCT.
- Las cuentas de proveedores y usuarios externos deben ser de perfiles específicos y tener caducidad no superior a tres (3) meses, renovables de acuerdo a la naturaleza del usuario.
- Los proveedores y usuarios externos deben aceptar por escrito los términos y condiciones de uso de la información y recursos de TI del Ministerio.

A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

A.16.1 Gestión de incidentes y mejoras en la seguridad de la información

- La Oficina TIC deberá definir los lineamientos para:
  - Responsables de la gestión de incidentes de seguridad de la información.
  - Los canales para que los colaboradores del MVCT puedan reportar los incidentes de seguridad de la información.
  - Para la evaluación de eventos de seguridad de la información y la decisión tomada sobre los mismos.
  - Para la recolección de evidencia de incidentes de seguridad de la información.
- La Oficina TIC deberá contar con los mecanismos para el cumplimiento de los tiempos en la respuesta de incidentes establecido en los lineamientos para la gestión de incidentes.
- La Oficina TIC deberá proporcionar los medios para el aprendizaje al MVCT de los incidentes de seguridad de la información.
- La Oficina TIC deberá dar a conocer a los colaboradores del MVCT, los lineamientos establecidos para la gestión de incidentes de seguridad de la información.

- Los funcionarios del MVCT deben reportar con diligencia, prontitud y responsabilidad presuntas violaciones de seguridad de la información a través del Jefe de dependencia al Líder del sistema de gestión de seguridad de la información "Jefe de la Oficina TIC", quienes deben garantizar las herramientas informáticas para que formalmente se realicen tales reportes.
- El MVCT a través de la Oficina TIC o del proveedor de servicios, podrá monitorear el tráfico en la red para administrar eficientemente los servicios de red, el ancho de banda, anticiparse a posibles amenazas y velar por el cumplimiento de las políticas de seguridad de la información.
- Los siguientes pueden ser considerados incidentes de seguridad de la información:
  - Fraude y robo de activos de información o de cómputo.
  - Divulgación, manipulación, destrucción o modificación no autorizada de la información del Ministerio.
  - Interrupción de procesos y sistemas críticos del Ministerio.
  - Fallas en la seguridad de los sistemas de información.
  - Fallas en la seguridad física de las instalaciones.
  - Acceso no autorizado a los recursos del Ministerio.
  - Uso indebido de los privilegios dentro de un sistema.
  - Propagación de virus cibernéticos o código malicioso.
  - Intrusiones externas a la red (hackeo).
  - Instalación de software no autorizado, entre otros.
- Es responsabilidad de todos los funcionarios y contratistas del MVCT reportar cualquier tipo de incidente relacionado con la información y/o los recursos informáticos a la mayor brevedad posible.
- Cualquier intento de interferencia, obstrucción o de disuadir a quien reporta una posible violación de seguridad, está prohibido y será motivo de una acción disciplinaria. De igual manera cualquier retaliación o amenaza contra la persona que realiza la investigación.
- Toda falla aparente de cualquier sistema de información o software debe ser reportada a la Oficina TIC, en caso de tratarse de un sistema de información adquirido a terceros debe reportarse la falla al proveedor del software.
- Los reportes de los incidentes deberán ser lo más completo posibles, aportando la mayor cantidad de evidencias a fin de facilitar la atención del mismo. Opcionalmente los funcionarios podrán mantener el anonimato durante su reporte o denuncia.
- Todos los reportes deberán ser manejados con estricta confidencialidad.
- Queda prohibido divulgar cualquier información sobre un incidente de seguridad de la información a personal externo, a menos que por disposiciones legales el ministerio se vea obligado a hacerlo. de ser así, deberá ser bajo la aprobación de la Alta Dirección del Ministerio y el Comité Institucional de Gestión y Desempeño.
- El funcionario o contratista que por negligencia no reporte a tiempo un incidente de seguridad o que aproveche deficiencias de seguridad y haga mal uso de la información, será investigado por el Grupo de Control Interno

Disciplinario para establecer las sanciones disciplinarias a que haya lugar.

- Los incidentes de seguridad de la información que estén relacionados con requerimientos legales o regulatorios deberán ser reportados a autoridades externas por personal autorizado del MVCT.
- Después de recibida la notificación de un incidente de seguridad o vulnerabilidad de la información, el gestor de incidentes es responsable de asegurar que el propietario del activo de información y todas las personas involucradas con el incidente, estén informadas.
- Todos los incidentes de seguridad deben ser evaluados de acuerdo con su circunstancia particular; esto puede requerir o no la acción de varias áreas del Ministerio. Cuando lo requiera la gravedad del incidente de seguridad el Grupo de Control Interno Disciplinario iniciará un proceso disciplinario para establecer las sanciones disciplinarias a partir de la falta cometida.
- Los incidentes de seguridad de la información deben ser investigados por personal calificado. Es necesario identificar las causas y planear como prevenir su reincidencia.
- La Oficina TIC deberá crear bases de datos de incidentes con sus respectivas soluciones para que permitan reducir el tiempo de respuesta en caso de ocurrencia de nuevos incidentes.

A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO

A.17.1 Continuidad de seguridad de la información

- La Oficina TIC deberá definir los lineamientos de seguridad de la información que se deben seguir prestando mientras el Ministerio opere bajo estrategias del plan de continuidad del negocio.
- La Oficina TIC deberá diseñar una herramienta para el análisis de impacto al negocio tecnológico del ministerio, por medio del cual se identifiquen los servicios críticos de tecnología del Ministerio.
- La Oficina TIC deberá diseñar estrategias de recuperación de los servicios críticos de tecnología.
- Cada servicio tecnológico identificado como critico o esencial deberá contar con planes de contingencia.
- La Oficina TIC deberá identificar los escenarios y las estrategias del plan de recuperación tecnológica DRP de los servicios esenciales de tecnología identificados.
- Todas las estrategias de recuperación tecnología deben contemplar los requisitos de seguridad de la información descritos en el presente manual.
- El plan de recuperación tecnológica y los planes de contingencia de los servicios de tecnología deberán se probados como mínimo una vez al año.
- Los procesos que sean desarrollados por terceros deberán disponer de planes de contingencia y se deberá analizar su cobertura.
- Se 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.

- Se debe establecer un programa de pruebas, teniendo en cuenta los requerimientos técnicos necesarios. Las pruebas deberán ejecutarse de manera que simule las condiciones de un evento y no se afecte la operación.
- Se deben documentar las pruebas y se deben generar reportes o informes después de cada prueba y/o ejercicio que incluya recomendaciones, lecciones aprendidas y acciones para mejorar el plan de recuperación tecnológica.
- 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 recuperación tecnología se mantenga actualizado y mejorado.
- La Oficina TIC deberá revisar y aprobar todos los planes.

A.17.2 Redundancias

- La Oficina TIC deberá contar con sistemas redundantes para los servicios críticos del Ministerio con el fin de garantizar la disponibilidad de los mismos.
- La Oficina TIC deberá poner a prueba los componentes o arquitecturas redundantes implementadas para asegurar que después de una falla el componente funcione.

A.18 CUMPLIMIENTO

A.18.1 Cumplimiento de requisitos legales y contractuales

- La Oficina TIC deberá identificar, documentar y actualizar la legislación referente a seguridad de la información en el normograma de la Oficina TIC.
- La Oficina TIC deberá definir controles con el objetivo de proteger adecuadamente la propiedad intelectual tanto propia como la de terceros, tales como derechos de autor de software, licencias y código fuente.
- La Oficina TIC deberá generar conciencia a los colaboradores del MVCT sobre 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.
- El Grupo de Atención al Usuario y Archivo y la Oficina TIC deberán definir y establecer:
  - Directrices sobre retención, almacenamiento, manipulación y eliminación de registros e información física y digital.
  - Deberá establecer e implementar controles para proteger los registros contra pérdida, destrucción y falsificación de información física y digital.
  - Deberá establecer procedimientos de almacenamiento a largo plazo y manipulación de los registros físicos y digitales.
- El MVCT deberá tomar todas las precauciones para conservar la confidencialidad y la integridad de todos los datos de carácter personal que la

entidad conserve de funcionarios, contratistas o terceros, almacenados o archivados en cualquier medio, entre otros están: cualquier información numérica, alfabética, gráfica, fotográfica, audiovisual o de cualquier otro tipo concerniente a personas físicas identificadas o identificables. Se deben adoptar los controles necesarios como lo exigen la Ley 1581 de 2012 y el Decreto 1377 de 2013, para prevenir incidentes de seguridad relacionados con la información personal que conserve el Ministerio en cualquier forma de almacenamiento.

- Todos los funcionarios y contratistas deberán conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan acceso con motivo del ejercicio de sus funciones. El Ministerio redactará un "Compromiso de Confidencialidad", el cual deberá ser suscrito por todos los funcionarios y contratistas que tengan acceso a información clasificada o reservada. La copia firmada del compromiso será retenida en forma segura por el Ministerio.
- Mediante este instrumento el subscriptor se comprometerá a utilizar la información solamente para el uso específico al que está destinada y a no comunicar, diseminar o de alguna otra forma hacer pública la información a ninguna persona, firma, compañía o tercera persona, salvo autorización previa y escrita del responsable del activo de que se trate. El "Compromiso de Confidencialidad" deberá especificar que determinadas actividades pueden ser objeto de control y monitoreo.
- Por regla general toda obra (incluido el software), patente, modelo de utilidad, diseño industrial, marca, logotipo, base de datos, etc., relacionados con los procesos del MVCT, que se desarrollen de manera colectiva y/o individual, bajo las políticas y directrices institucionales, son propiedad del MVCT, su uso es considerado restringido para los fines de la misión y deberá ser protegido de otro descubrimiento o uso que menoscabe la reputación del MVCT.

En consecuencia:

Los funcionarios y contratistas están obligados a poner en conocimiento de sus jefes tales elementos de desarrollo, realizado con recursos del MVCT y a transferir de manera solemne, cuando por ley se requiera, todos los derechos que se deriven de los mismos a favor del MVCT.

Las personas contratadas por el MVCT para la prestación de servicios de desarrollo de software, deberán garantizar la propiedad de los derechos patrimoniales sobre el software contratado en cabeza del MVCT.

Para estos efectos los contratos deberán:

- Ser por escrito entre autor y MVCT y en ellos se pactará la remuneración.
- Indicar que se elaboran por cuenta y riesgo del MVCT.
- Todos los desarrollos serán de propiedad del MVCT y este conservará todos los derechos incluyendo los de autor sobre estos desarrollos.
- Establecer el plan señalado por el MVCT determinando condiciones de necesidad, características y atributos de la obra, y estableciendo los lineamientos de tiempo, modo y lugar para su desarrollo.

A.18.2 Revisiones de seguridad de la información

- 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.

- 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 tomarán las acciones necesarias, conforme a lo establecido en el procedimiento SMC-P-05, acciones preventivas, correctivas y de mejora, a fin de documentarlas en el Sistema Integrado de Gestión.
- La Oficina TIC, como segunda línea de defensa y líder de la política de seguridad digital realizará monitoreo o seguimiento periódico 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.
- La Oficina de Control Interno realizará evaluaciones independientes basadas en las muestras de los sistemas de información y al SGSI del MVCT, con un enfoque en riesgos de seguridad digital, de acuerdo a lo establecido en su Plan Anual de Auditorías y a la disponibilidad de los recursos necesarios para su ejecución conforme a las necesidades y expectativas de la Alta Dirección, teniendo en cuenta los resultados de las auditorías realizadas por la segunda línea de defensa.

A.19 POLITICA SEGURIDAD DE DATOS

En cada uno de los apartados descritos anteriormente, hay un componente de información que se considera y se han definido lineamientos de seguridad de la información específicos a cada uno en el alcance del componente desarrollado, por ejemplo, para el uso de equipos de cómputo personal, dispositivos móviles uso del correo electrónico, etc. se definieron políticas y lineamientos de seguridad de la información. Las políticas y lineamientos descritos a continuación complementan las definidas anteriormente para cada tema en específico.

A.19.1 Estándares para la seguridad de datos

- La Oficina TIC deberá definir estándares, que cubran los siguientes aspectos:
  - Herramientas usadas para la seguridad de datos
  - Estándares y mecanismos de cifrado de datos.
  - Guías para el acceso seguro de usuarios externos e internos.
  - Protocolos de transmisión de datos sobre la red de Internet.
  - Estándares de acceso remoto.
  - Procedimientos de reporte de incidentes de seguridad.

A.19.2 Controles y procedimientos para la seguridad de datos

- La seguridad de las bases de datos es una responsabilidad de los administradores de las mismas.
- El administrador de la base de datos "DBA" debe gestionar los roles y privilegios sobre las instancias, estructuras de datos y datos.

- El acceso a las bases de datos se debe dar de acuerdo con los procedimientos de atención derequerimientos definidos por la entidad y este acceso debe ser documentado en el caso.
- En caso de que se requiera la modificación de datos en las bases de datos de la entidad, este solamente puede darse, luego de la gestión y aprobación de un control de cambios que debe documentar, el solicitante, área de la entidad, jefe directo, datos anteriores y nuevos a ser ajustados y un documento de soporte del área solicitante, puede ser memorando por parte del jefe responsable /dueño de la información.

A.19.3 Gestión de usuarios y claves para la seguridad de datos

- Los permisos de acceso y actualización a los datos se deben dar a nivel de cuenta, sin embargo,de acuerdo con el volumen y complejidad de los accesos se pueden definir grupos, previa validación con el oficial de seguridad de la información.
- En el caso de existir grupos para el acceso a los datos, los usuarios solo pueden pertenecer a un solo grupo.
- Los administradores de las bases de datos "DBAs", son los responsables de la creación, modificación y eliminación de las cuentas de usuario para el acceso a los datos.
- En caso de que se requiera la creación de una cuenta de servicio/aplicación esta debe tener asignado/documentado una persona como responsable, puede ser el líder técnico o funcional de la aplicación o servicio.
- Se debe definir una taxonomía para la gestión de las cuentas de usuario, en caso de cambiarseesta, se debe acordar con el oficial de seguridad de la entidad.
- Todas las cuentas de usuario/servicio deben ser protegidas con una clave que cumpla los estándares de complejidad definidos.
- No se permite el uso de claves en blanco.
- No se permite el uso de claves iguales al nombre de usuario o cuenta.

A.19.4 Gestionar Vistas de datos y permisos

- El control de acceso a las vistas de datos se debe dar a nivel de usuario o grupo.
- Ninguna vista de datos debe contemplar el acceso sin restricción.
- Los grupos de interés en conjunto con el administrador de la base de datos "DBA", deben definirlos campos requeridos en la vista y únicamente estos deben ser incluidos en ella.
- En caso de que se requiera el acceso remoto a una vista, este acceso se debe dar a través deun mecanismo seguro, como una VPN S2S.

A.19.5 Auditoría de la Seguridad de los datos

- Se debe implementar una herramienta que permita la auditoría de seguridad de los datos.
- Se debe evaluar la pertinencia de habilitar la auditoria a un conjunto de datos determinando,considerando la pertinencia, impacto en el procesamiento y los

requerimientos técnicos.

- La auditoría en las bases de datos se debe habilitar de acuerdo con las necesidadesidentificadas y se deben generar reportes de auditoría.

14. CONTROL DE CAMBIOS

Fecha	Versión del documento que modifica	Versión actual del documento	Motivo de la modificación
06-06-2020	1.0	**2 .0**	Actualización de introducción, objetivo general, alcance, compromiso de la alta dirección, competencia, roles y responsabilidades, matriz de comunicaciones y partes interesadas.
14-12-2021	2.0	3.0	Definición de las competencias en formación y experiencia del oficial de seguridad de la información y de los colaboradores responsables de la sostenibilidad y mejoramiento del sistema de gestión de seguridad de la información – SGSI, Actualización de lineamientos generales de las políticas de tercer nivel A.6.3, A.7.1, A.7.2, A.7.3, A.8.1, A.8.2, A.8.3, A.9.1, A.9.2, A.9.3, A.9.4, A.10.1, A.11.1, A.11.2, A.12.1, A.12.2, A.12.3, A.12.4, A.12.5, A.12.6, A.12.7, A.13.1, A.13.2, A.14.1, A.14.2, A.14.3, A.15.1, A.15.2, A.16.1, A.17.2 y , A.18.2; Los cuales fueron concertados a través de mesas de trabajo con algunas dependencias del Ministerio Se adiciono el numeral A.19 POLÍTICA SEGURIDAD DE DATOS

09-08-2023	3.0	4.0	Se ajusto numeración, por cuanto el numeral 10 no existía. Se incluyo numeral 12.2.11 Política de manejo de información de los servidores de la entidad frente a terceros