**Ministerio de Vivienda Ciudad y Territorio**

# MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDADDE LA INFORMACIÓN Y SEGURIDAD DIGITAL

**2024**

## TABLA DE CONTENIDO

# 1. INTRODUCCIÓN

Las exigencias de seguridad requeridas actualmente frente al esquema de globalización de las tecnologías 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 contra la 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 27001:2022 y en el código de buenas prácticas para la gestión de la seguridad de la información ISO/IEC 27002:2022 y en el Modelo de Seguridad y Privacidad de la Información MSPI.

# 2. OBJETIVOS

## 2.1. OBJETIVO GENERAL

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

## 2.2. OBJETIVO ESPECÍFICOS

- Definir los roles y responsabilidades para la implementación, seguimiento y mejora del SGSI.
- Sensibilizar sobre los requerimientos técnicos del estándar ISO/IEC 27001:2022 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.
- 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 (Ministerio de Vivienda, Ciudad y Territorio), 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. 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 coordinar esfuerzos entre funcionarios y/o contratistas de las diferentes dependencias del Ministerio para 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.

## 5. COMPROMISO DE LA ALTA DIRECCIÓN

El Ministro (a) 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.

## 6. COMPETENCIA

La sostenibilidad y mejora 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, según su papel.

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 27001:2022, 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.

## 7. ¿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.

## 7.1. 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, según el artículo tercero de la resolución 0958 del 24 de diciembre de 2019, del que se desprenden las responsabilidades referidas 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(a) Ministro (a) 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 DE LA IMPLEMENTACIÓN, SEGUIMIENTO Y MEJORA DEL SGSI

El Líder del SGSI, es el Jefe (a) 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. Revisar periódicamente las políticas de seguridad de la información o cuando ocurran cambios significativos.
6. Asesorar técnicamente a otros procesos en temas relacionados con el SGSI.
7. Determinar la necesidad de cambios del SGSI.
8. Liderar la gestión de riesgos de seguridad de la información y seguridad digital en coordinación con la Oficina Asesora de Planeación.
9. 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.
10. Realizar las acciones y gestiones necesarias para el cumplimiento de la política y los objetivos del SGSI.
11. 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.
12. Realizar seguimiento a la gestión de incidentes de seguridad de la

información.
13. Reportar, ante la instancia orientadora del sistema, los incidentes catalogados como catastróficos.
14. Aprobar los indicadores del SGSI.
15. Aprobar los informes y reportes relacionados con el SGSI, que soliciten los entes de control y demás partes interesadas internas y externas del Ministerio.
16. 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.
17. Coordinar, retroalimentar y representar al equipo técnico responsable de implementar el SGSIante las diferentes instancias, y revisar anualmente su conformación.
18. Monitorear y realizar seguimiento a la implementación del SGSI.
19. 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 (a) 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. Monitorear y actualizar permanentemente las advertencias relativas a las amenazas de seguridad, para ser analizadas, y así anticipar estas amenazas y riesgos, permitiendo una mejor toma de decisiones y una respuesta eficaz.
6. 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
7. Asesorar técnicamente a otros procesos en temas relacionados con seguridad de la información.
8. Elaborar el plan de acción del SGSI.
9. Proponer cambios al SGSI.

10. Realizar campañas de concienciación en temas referentes a seguridad de la información al interior del Ministerio.
11. 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.
12. 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.
13. Actualizar la documentación del SGSI.
14. Establecer y apoyar en la implementación de los controles tecnológicos de seguridad de la información en el Ministerio.
15. Consolidar la matriz de activos de seguridad de la información.
16. Comunicar los incidentes de seguridad de la información al Líder del sistema.
17. 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.
18. 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.
19. Las demás asignadas por el Líder del sistema de gestión de seguridad de la información.

### 7.3.2. Competencias en Formación y Experiencia del Oficial de Seguridad de la Información

El Oficial de Seguridad de la Información del MVCT deberá poseer la siguiente formación y experiencia mínima:

- Título de formación profesional en: Ingeniería de Sistemas y afines, ingeniería Telemática y afines, o Ingeniería Electrónica y afines.
- Título de formación de especialización o de maestría relacionada con seguridad de la Información.
- Conocimiento en auditoría de sistemas de información o seguridad de la información.
- Experiencia profesional de al menos dieciocho (18) meses en áreas afines a la seguridad de la información, abarcando aspectos como, seguridad informática, auditoría de sistemas de información y comunicación
- Conocimientos sólidos en la gestión de riesgos y en la implementación de controles de seguridad de la información.

## 7.4. SERVIDORES PÚBLICOS DEL MINISTERIO

### 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 los jefes y/o delegados de los siguientes procesos:

- Gestión de las Tecnologías de la Información y las Comunicaciones,
- Direccionamiento Estratégico
- Gestión de Recursos Físicos
- Gestión Documental
- Gestión Estratégica del Talento Humano
- Gestión de Contratación
- Conceptos Jurídicos

El proceso de Evaluación, Independiente y Asesoría, 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 de este 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.

### 7.4.1 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.

#### 7.4.1.1 Responsabilidades de los Líderes de los Procesos

Las responsabilidades de los lideres de los procesos en SGSI, son permanentes así se hayan delegado en cualquier otro colaborador del MVCT; dentro de la cuales se encuentran:

1. Gestionar (elaborar, modificar, eliminar, socializar e implementar) la documentación de su proceso, teniendo en cuenta las políticas y/o lineamientos de seguridad de la información.
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, siguiendo lo definido en la Metodología Integrada de Administración del Riesgo definida por el Ministerio.
5. Velar por cumplir las políticas y directrices definidas en la implementación del Sistema de Gestión de Seguridad de la Información, al interior de cada dependencia que conforman los procesos del Sistema Integrado de Gestión del Ministerio.
6. Mitigar el riesgo de fraudes, errores y abusos, tanto intencionales como no intencionales, asignando las responsabilidades y las tareas críticas del proceso entre diferentes colaboradores, de manera que un solo colaborador no tenga un control completo sobre una actividad o proceso de importancia significativa.
7. Las demás que conforme a las disposiciones legales puedan desarrollar.

### 7.4.2. Lideres de las Políticas Especificas

Se denomina líder de las políticas específicas, al cargo, responsable de desarrollar políticas de seguridad de la información que sean específicas para las necesidades y contextos particulares del Ministerio de Vivienda, Ciudad y Territorio.

### 7.4.3. Colaboradores Ministerio

Este rol lo conforman todos los colaboradores (funcionarios y contratistas) que hacen parte del Ministerio de Vivienda, Ciudad y Territorio.

## 8. RESPONSABILIDADES DE LOS COLABORADORES

1. Proteger la información institucional y los activos de información asociados a esta, cumpliendo y acatando las políticas y/o lineamientos que se dicten en materia de seguridad de la información.
2. Participar en las actividades de concienciación que se realicen en el marco del SGSI.
3. Reportar los incidentes 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 estos.

### 8.1. GRUPOS 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.

## 9. COMUNICACIÓN

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 locomunica? | ¿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 2014 | Oficial de Seguridad de la Información | Profesional que lidera la política de transparencia de la entidad | Anual | Página web |
| 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 o Tips 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 |
| Lineamientos y directrices del manual de políticas de seguridad y privacidad de la información y seguridad digital | Oficial de Seguridad de la Información | Líderes de los procesos | Cuando se requiera | correo electrónico y comunicaciones escritas |

## 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 de la 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 Ministerio. | 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 Ministerio. | Manual Políticas de Seguridad de la Información. | Reducción de probabilidad de afectación a la información que custodie. |
| Usuarios | Protección de la información suministrada al Ministerio. | Cumplimiento de las políticas de Seguridad de la Información reduciendo las probabilidades de afectación a la información del Ministerio. | Manual Políticas de Seguridad de la Información. | Reducción de probabilidad de afectación a la información de los usuarios del Ministerio. |
| 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. Proteger, preservar y administrar la integridad, confidencialidad, disponibilidad y autenticidad de la información suministrada al Ministerio. | Cumplir las políticas de Seguridad y privacidad de la Información, con el propósito de preservar la información custodiada por el Ministerio. | Manual Políticas de Seguridad de la Información. | Reducción de probabilidad de afectación a la información de la sociedad y de la comunidad. |

| Parte interesada | Necesidades | Expectativas | Requisitos en el sistema de gestión | Logros y resultados esperados |
|---|---|---|---|---|
| **GOBIERNO** | | | | |
| 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 Ente | Manual Políticas de Seguridad de la Información. | Respuesta oportuna a incidentes de Seguridad de la Información que contemplan 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 delnegocio. | 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. |

| Parte interesada | Necesidades | Expectativas | Requisitos en el sistema de gestión | Logros y resultados esperados |
|---|---|---|---|---|
| **ALIADOS ESTRATEGICOS** | | | | |
| 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 Ministerio 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 trámites en 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 Ministerio se dividen en tres (3) niveles, los cuales se definen según su orden de importancia en:

## 11.1. 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 se alinea con las normas internacionales ISO 27000 para gestionar la seguridad de la información y con el PETI–plan estratégico de TI del Ministerio de Vivienda, Ciudad y Territorio y se define en la resolución que establece el SGSI en el Ministerio.

## 11.2. 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.

### 11.3. TERCER NIVEL

Corresponde a **Políticas Específicas de Seguridad de la información**, enfocadas a grupos, servicios o actividades particulares. Estas políticas o lineamientos resumen los aspectos más relevantes en seguridad de la información para el Ministerio hacen parte del presente manual como una guía de aplicación definida en el SIG y su definición está alineada con los controles específicos establecidos en la norma internacional ISO 27001:2022.

## 12. POLITICAS DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO.

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.

### 12.1. 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 Ministerio 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. 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 Ministerio. Esta política aplica a los dispositivos electrónicos personales, como teléfonos inteligentes y tabletas, a los ordenadores portátiles que no pertenecen al Ministerio, pero que usan 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).

## 12.3. 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 aplicarse por los funcionarios y/o contratistas que realicen teletrabajo y/o trabajo remoto.

## 12.4. 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 ellos, para protegerlos de accesos no autorizados.

Esta política debe aplicarse por los funcionarios, contratistas y terceras partes que acceden a los activos de información del Ministerio.

## 12.5. 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 esta.

## 12.6. POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIOS.

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 aplicarse por los funcionarios, contratistas y terceras partes que acceden a los activos de información del Ministerio.

## 12.7. POLÍTICA RESPALDO DE LA INFORMACIÓN

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

Esta política debe aplicarse por los funcionarios, contratistas y terceras partes que acceden a los activos de información del Ministerio.

## 12.8. 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.

## 12.9. POLÍTICA DE PROTECCIÓN DE LA PROPIEDAD INTELECTUAL

La Propiedad Intelectual en Colombia está protegida por la Constitución Política (artículo 61) como derecho fundamental y establece la obligación del estado de protegerla. De esta forma se creó la Ley de Derecho de Autor, Ley 23 de 1982 (modificado por la Ley 2294 de 2023), siendo complementada por la Ley de Propiedad Industrial (Ley 603 de 2000) y las Decisiones 291/1991, 391/1996 y 486/2000 de la Comunidad Andina de Naciones.

Al incorporar procedimientos y abordar los requisitos relativos a la Propiedad Intelectual, se asegura que el MVCT cumpla con todos los requisitos de propiedad intelectual y derechos de autor. Esto implica la reducción de cualquier riesgo de seguridad asociado con el incumplimiento de estos requisitos por parte de la entidad y sus colaboradores.

Los beneficios que ofrece tener una política centrada en la Protección de los Derechos de Propiedad Intelectual son:

1. Condición indispensable incluida en la normativa ISO 27001:2022.
2. Mejora de la Seguridad de la Información: Al implementar eficazmente los protocolos de seguridad de la información, se asegura de cumplir con los requisitos externos establecidos por leyes, reglamentos, estatutos y contratos, fortaleciendo así la seguridad en todos los niveles.
3. Reducción de Riesgos en Seguridad de la Información: Al cumplir con los requisitos y obligaciones externos, se reduce significativamente el riesgo de brechas en la seguridad de la información, disminuyendo la probabilidad de eventos no deseados.
4. Mejora del Cumplimiento Normativo: Cumplir con estándares y regulaciones es una exigencia en diversos contextos. La implementación de los requisitos externos fortalece y garantiza un cumplimiento más robusto y efectivo de la normativa ISO 27001.
5. Protección de la Reputación Organizacional: Contar con una sólida Política de Protección de Propiedad Intelectual, minimiza el riesgo de sanciones, y además reduce el impacto en las relaciones públicas, preservando la reputación de la entidad.

A partir de la creación de una obra en Ministerio, surge en cabeza del titular o del autor dos grandes tipos de derechos, los Derechos Morales, y los derechos Patrimoniales.

Los derechos morales son definidos como el vínculo moral y espiritual, entre el autor y su obra, y tienen carácter inalienable e irrenunciable. Los derechos patrimoniales se denominan como tal, porque hacen parte del patrimonio del autor, por lo que se traducen en la facultad de beneficiarse y disponer de su obra.

El Ministerio para los procesos de contratación, adquisición, desarrollo de proyectos o acuerdos de desarrollo de software, investigación, cooperación y otros convenios con contratistas, consultores, proveedores, investigadores, universidades, organismos internacionales, así como personas de carácter público o privado, requiere la consideración cuidadosa de los siguientes elementos:

a. Establecer, desde la fase inicial de los procesos de contratación, convenios o acuerdos, los términos relativos a la titularidad de la propiedad intelectual.
b. Definir los activos de propiedad intelectual derivados del objeto contractual, junto con los mecanismos contemplados en la legislación aplicable para la generación de derechos sobre estos activos, de acuerdo con su clasificación.
c. Reservar y justificar la titularidad de la propiedad intelectual o el derecho de registrarla a nombre del Ministerio, u optar por el licenciamiento de los derechos generados o adquiridos durante la ejecución.

El Ministerio ostentara la titularidad de los derechos patrimoniales de autor en los siguientes casos:

1. Cuando las obras son generadas por colaboradores vinculados al Ministerio.
2. En el caso de obras realizadas por contratistas y terceros como parte de sus obligaciones contractuales y funciones para las cuales fueron contratados.
3. En situaciones donde las obras resultan de procesos creativos o de investigación llevados a cabo en la ejecución de contratos o convenios específicos, suscritos con el Ministerio, con el propósito de desarrollar obras científicas, literarias, artísticas o de software.
4. En relación con obras coordinadas, divulgadas, publicadas y/o editadas por el Ministerio.

Los aspectos mencionados anteriormente, con la excepción del primero, serán convenidos a través de un contrato debidamente formalizado. Este contrato establecerá las condiciones de producción, con el Ministerio asumiendo los riesgos asociados. Además, se especificarán las contraprestaciones acordadas y se diseñará un plan detallado para la elaboración de la obra antes de su ejecución.

### 12.9.1. Protección de los Derechos de Propiedad Intelectual del Software

Se definen los siguientes lineamientos que buscan la protección de los derechos de propiedad intelectual del software utilizado en el Ministerio:

1. La adopción de software se regirá por un análisis crítico, riguroso y adaptado a las necesidades, priorizando beneficios, eficiencia y eficacia en el soporte de los procesos institucionales.
2. Todo software utilizado en equipos del Ministerio debe cumplir con principios constitucionales, acuerdos internacionales y legislación nacional de derechos de autor, respetando los términos de licenciamiento.
3. La instalación de software en equipos debe realizarse y utilizarse conforme a los términos de licenciamiento.
4. El software se considera un activo institucional por tanto este debe ser inventariado.
5. Se deberá mantener un repositorio centralizado, asegurando respaldo y copias de seguridad para gestionar eficientemente los activos de software.
6. Los usuarios deben:
   a. ser informados de las capacidades del licenciamiento del software en uso, aclarando que cosas están permitidas y cuáles no.
   b. ser advertidos sobre las consecuencias de la violación de las políticas de uso legal de software.

## 12.10. POLÍTICA DE DESARROLLO DE SOFTWARE

Cuando el Ministerio de Vivienda, Ciudad y Territorio, desarrolle software o contrate software con proveedores, deberá considerar los lineamientos generales para desarrollar, mantener y adquirir software, que defina la OTIC para adoptar 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.

## 12.11. 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 Ministerio, cuando se autorice el acceso o administración por parte de proveedores de servicios o contratos de prestación de

servicios.

## 12.12. 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.

## 12.13. POLITICA SEGURIDAD DE DATOS

Las políticas y lineamientos descritos a continuación complementan las definidas anteriormente para cada tema en específico.

### 12.13.1. Estándares para la seguridad de datos

- La OTIC 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.

### 12.13.2. Controles y procedimientos para la seguridad de datos

- La seguridad de las bases de datos es una responsabilidad de los administradores de estas.
- 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 de requerimientos definidos por la entidad y este acceso debe ser documentado en el caso.
- Si se requiere modificar datos en las bases de datos de la entidad, solo puede darse, tras 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 ajustar y un documento de soporte del área solicitante, puede ser memorando por el jefe propietario de la información.

### 12.13.3. 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.
- Si se requiere crear 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 cambiarse esta, 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.

### 12.13.4. 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 definir los campos requeridos en la vista y únicamente estos deben ser incluidos en ella.
- Si se requiere el acceso remoto a una vista, este acceso se debe dar a través de un mecanismo seguro, como una VPN S2S.

### 12.13.5. 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 necesidades identificadas y se deben generar reportes de auditoría.

## 13. OBSERVACIÓN REFERENTE A LA NUMERACIÓN DE LOS CONTROLES APLICABLES

Las numeraciones de las políticas específicas de seguridad de la información en el Anexo No2 a continuación, conservan su numeración de acuerdo con el anexo A de la norma ISO: 27001:2022

Los controles 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.

ANEXO No.1

# ANEXO No.1

## POLÍTICAS DE ESPECIFICAS

## GUIA DE APLICACIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ANEXO No.1

## A.5 CONTROLES ORGANIZACIONALES

### A.5.1 Políticas de seguridad de la información

- Las políticas de seguridad de la información y las políticas específicas de la Seguridad de la Información son las dispuestas en el numeral *12. POLITICAS DE SEGURIDAD DE LA INFORMACIÓN DEL MVCT*, del Manual de Políticas Generales.
- El Líder del sistema de seguridad de la información y los responsables de las políticas específicas deberán darlas a conocer a todos los colaboradores del MVCT y las partes interesadas cuando se requiera.
- La política general y las políticas específicas deben ser revisadas una vez al año o cuando haya cambios significativos.

### A.5.2 Roles y responsabilidades de seguridad de la información

- 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.
- ElLíder del sistema de seguridad de la información debe dar a conocer los roles y responsabilidades a todos los colaboradores del Ministerio.

### A.5.3 Segregación de deberes

Según la norma ISO 27001, el Anexo A Control A.5.3 describe las directrices para la segregación de tareas y funciones de la organización.

La segregación de tareas y funciones de la organización, al delegar subprocesos en diferentes personas, crea un sistema de controles y equilibrios que reduce la probabilidad de errores y fraudes. Este control evita que una sola persona cometa, oculte y justifique acciones indebidas, reduciendo el riesgo de fraude y error, y evitando que anule los controles de seguridad de la información.

En situaciones donde un único colaborador tiene todos los derechos necesarios para llevar a cabo un proceso, existe un mayor riesgo de fraudes y errores. Esto se debe a que un solo colaborador puede realizar todas las tareas sin ningún tipo de control. Sin embargo, al no asignar a un solo colaborador todos los derechos de acceso necesarios para un proceso específico, se reduce el riesgo de que este cause daños significativos o pérdidas a la información.

- La información deberá estar bajo la responsabilidad del Líder de proceso, quien realizará Segregación de Deberes, para prevenir y detectar irregularidades en los activos de información del MVCT, tal como está dispuesto en el numeral *7.4.4.1 RESPONSABILIDADES DE LOS LIDERES DE PROCESOS* del presente manual.

- Los procesos que impliquen actividades sobre los activos de la información deberán tener segregación de deberes. Entre estas actividades se encuentran:
    a) iniciar, aprobar y ejecutar un cambio;
    b) solicitar, aprobar y aplicar derechos de acceso;
    c) diseñar, implementar y revisar código;
    d) desarrollar software y administrar sistemas de producción;
    e) utilizar y administrar aplicaciones;
    f) utilizar aplicaciones y administrar bases de datos;
    g) diseñar, auditar y garantizar los controles de seguridad de la información.

**A.5.4 Responsabilidades de gestión**

Las responsabilidades de la alta dirección deben incluir asegurar que:

- El Grupo de Talento Humano y el Grupo de Contratación son responsables de informar a los colaboradores en los términos y condiciones de empleo o contrato, los roles y responsabilidades relacionados con la seguridad de la información antes de acceder a la información del Ministerio y otros activos asociados.
- La oficina OTIC apoyará en los temas referentes al SGSI en las reuniones de inducción y reinducción a los colaboradores.

**A.5.5 Contacto con autoridades**

- El Líder del sistema de seguridad de la información deberá mantener contacto con las autoridades nacionales 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 Ministerio. Estos deberán ser divulgados a los colaboradores del Ministerio.

**A.5.6 Contacto con grupos de interés especial**

- El Líder del SGSI deberá contactar con los grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales para contactarlos oportunamente si se presenta un incidente de seguridad de la información, que requiera de asesoría externa.

**A.5.7 Inteligencia de amenazas**

- El Equipo de Seguridad tiene la responsabilidad de requerir al administrador de la plataforma tecnológica de la entidad que proporcione informes de monitoreo y detección de amenazas en curso. Asimismo, deberá estar atento a la posible necesidad de establecer un nuevo perfil de riesgo digital y comunicarlo de inmediato al líder de seguridad.

- El oficial de seguridad solicitará al administrador de la plataforma el análisis y las recomendaciones de las advertencias sobre las amenazas de seguridad, que deberán obtenerse y analizarse para producir Inteligencia de Amenazas. Tras el análisis, se comunicarán las recomendaciones y las conclusiones principales a las partes interesadas relevantes. Además, se debe establecer un intercambio de información con las partes interesadas.
- La OTIC debe implementar una herramienta tecnológica que permita la detección y mitigación de diversas amenazas, como parte de su estrategia para garantizar la disponibilidad de la infraestructura. Esta herramienta facilitará la identificación y neutralización de posibles amenazas a la infraestructura.

### A.5.8 Seguridad de la información en la gestión de proyectos

- Los líderes de los procesos deben llevar a cabo una evaluación de riesgos de seguridad de la información en todos los proyectos que se implementen en su ámbito.
- La Oficina Asesora de Planeación, junto al Grupo de Contratos, se encarga de crear una guía de adquisición de bienes y servicios que abarque los aspectos vinculados a los sistemas de gestión adoptados por la entidad.
- La OTIC 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. Lo anterior cumpliendo con los lineamientos establecidos en el numeral A.8 Controles Tecnológicos

### A.5.9 Inventario de información y otros activos asociados

- El Líder del SGSI, o a quien este delegue, será responsable de aplicar y mantener actualizada la documentación para el levantamiento y actualización de los activos de información del Ministerio. Los Líderes de proceso se encargarán de identificar, clasificar y valorar los activos del MVCT utilizando el Formato de Registro de Activos de Información, definido en la Guía para la Gestión de Activos de Información del Ministerio. Este proceso deberá revisarse y actualizarse anualmente, o previo a los cambios

normativos vigentes, para garantizar la precisión y relevancia de la información sobre los activos de la organización.

- Los Líderes de los procesos del Ministerio, serán los propietarios de los activos de información identificados para sus procesos.
- Los Líderes de los procesos del Ministerio 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 físicos o digitales a los que estos se vean expuestos.
- 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 con la normativa vigente colombiana.

### A.5.10 Uso aceptable de la información y otros activos asociados

- La OTIC deberá establecer un documento donde se determine el uso aceptable de la información y los activos asociados, que considere entre otros los siguientes puntos:
  a) restricciones de acceso que respaldan los requisitos de protección para cada nivel de clasificación;
  b) mantenimiento de un registro de los usuarios autorizados de información y otros activos asociados;
  c) protección de copias temporales o permanentes de información a un nivel consistente con la protección de la información original;
  d) almacenamiento de activos asociados con la información de acuerdo con las especificaciones de los fabricantes.
  e) marcado claro de todas las copias de los medios de almacenamiento (electrónicos o físicos) para la atención del destinatario autorizado;
  f) autorización de eliminación de información y otros activos asociados y métodos de eliminación admitidos.

### A.5.11 Devolución de activos

- Al finalizar su empleo, contrato, convenio o acuerdo, los colaboradores y terceras partes deberán devolver todos los activos de información pertenecientes al Ministerio que tengan en su posesión. Estos activos pueden incluir dispositivos electrónicos, medios de almacenamiento o documentos físicos. Este proceso de devolución se realizará según los

procedimientos y políticas establecidas por el Ministerio para proteger los activos de la información y salvaguardar la confidencialidad de los datos.

- Al llegar al final de su ciclo de vida o por cualquier otro motivo que requiera la baja de los dispositivos electrónicos, la OTIC se encargará de proceder con un borrado seguro del disco para asegurar que los datos del Ministerio contenidos en estos dispositivos no puedan ser recuperados.
- Cuando se transfieran equipos de cómputo a otros colaboradores, la OTIC a través de la Mesa de Ayuda reinstalará el sistema operativo y los programas de la línea base.
- La OTIC será la única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro. Sin embargo, cuando se deba realizar desde y hacia el almacén, será el Grupo de Recursos Físicos el encargado, con el fin de mantener un control individual de inventarios. Es importante mencionar que toda reasignación de equipos deberá ajustarse a los procedimientos y competencias de la gestión de bienes del Ministerio.

### A.5.12 Clasificación de la información

El Ministerio a través del Grupo de Atención al Usuario y Archivo - GAUA, desarrollará los lineamientos para la clasificación de la información teniendo en cuenta lo siguiente:

- GAUA definirá los niveles adecuados para clasificación de la información de acuerdo con la normatividad colombiana vigente
- Estos niveles deberán ser oficializados y divulgados a todos los colaboradores.
- Los propietarios de la información se encargan de clasificar la información según los lineamientos definidos por GAUA.
- 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 Ministerio deberá tener un periodo de almacenamiento que puede darse por requerimientos legales o misionales; este periodo deberá indicarse en las tablas de retención documental y, cuando se cumpla el periodo de expiración, se eliminará o transferirá la información adecuadamente.
- El Ministerio, a través de GAUA y la OTIC deberán cumplir con los mecanismos necesarios para proteger la información catalogada como Información pública reservada, definidos por los propietarios de la información, independiente el medio en que se encuentren.
- 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 Ministerio.

- La información del Ministerio deberá protegerse incluso en los ambientes de pruebas.
- La información del Ministerio no debe divulgarse sin contar con los permisos correspondientes, además ningún funcionario, contratista o proveedor debe copiarla o extraerla cuando 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 propietario de la información.
- Los colaboradores que trabajen en sus equipos personales no deberán guardar en ellos información del Ministerio.
- Los colaboradores no deben divulgar información 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.5.13 Etiquetado de información

- El Grupo de Atención al Usuario y Archivo - GAUA deberá definir una Guía de Etiquetado para la información física y la información digital.
- Las series y subseries de las Tablas de Retención Documental (TRD) deberán contener en su estructura el tipo de clasificación.
- Cada Propietario de la Información velará por el cumplimiento establecido en la Guía de Etiquetado de la información

### A.5.14 Transferencia de información

- La Oficina de Control Interno - OCI en acompañamiento de la Oficina Asesora Jurídica (OAJ) deberán definir un documento de convenio de intercambio de información entre el MVCT y terceras que contenga entre otras:
    - La indicación que la información del MVCT no se puede copiar, modificar o compartir.
    - Una cláusula de confidencialidad y no divulgación de la información proporcionada.
- La OTIC deberá definir un procedimiento para el intercambio de información digital entre el Ministerio y terceras partes, considerando el estándar XROAD.
- Las dependencias del Ministerio que necesiten realizar transferencia de información con terceros deberán acoger el procedimiento definido por la OTIC.

- Se prohíbe la transferencia de información institucional sin la autorización del propietario.
- Se prohíbe la transferencia de información institucional a correos personales.
- El GAUA deberá definir el procedimiento para la transferencia de información física.
- Cuando se realice transferencia de información no estructurada (Word, Excel, Power Point, etc.), esta información deberá ser escaneada por el software antivirus con el fin de detectar código malicioso.
- La OTIC deberá establecer controles para proteger la información que se transmite como documentos adjuntos a través del correo electrónico del Ministerio.
- Los únicos repositorios autorizados para la transferencia de información son los definidos por la OTIC.
- 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 que cumpla con la política de controles criptográficos, esto debe quedar registrado en los convenios o acuerdos de intercambio de información que firmen las partes.
- El GAUA definirá directrices sobre retención de la información del MVCT, de acuerdo con la legislación y reglamentaciones locales y nacionales.
- El GAUA en compañía de la OTIC definirán las directrices sobre la disposición y transferencia de la información del Ministerio, de acuerdo con la legislación y reglamentaciones locales y nacionales.
- 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.
    - En caso de presentarse un incidente de seguridad de la información como la pérdida de un medio físico, se debe informar inmediatamente al Ministerio a través de la OTIC.
- Toda información enviada desde el Ministerio a través de correos electrónicos deberá incluir en su pie 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 Ministerio de Vivienda Ciudad y

Territorio, para el uso exclusivo de su destinatario. Si usted no 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 Ministerio entre su personal cuando dicho intercambio corresponda a actividades relacionadas con el desarrollo de sus actividades.

### A.5.15 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 Ministerio, el manejo que se les dé a las credenciales de acceso asignadas.
- El proveedor encargado de la gestión de la plataforma tecnológica del Ministerio, debe garantizar el acceso seguro a la misma.
- La conexión remota a la red de área local del Ministerio deberá establecerse a través de una conexión VPN suministrada por la OTIC.
- Las conexiones remotas deberán utilizar los métodos establecidos de autenticación para el control de acceso de los usuarios.
- La OTIC deberá implantar controles para el acceso por redes inalámbricas.
- La OTIC 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 OTIC deberá verificar periódicamente los controles de acceso para los usuarios del Ministerio y los provistos a terceras partes, para revisar que dichos usuarios tengan los permisos solo a los recursos de red y servicios de la plataforma tecnológica para los que se autorizaron.
- Los colaboradores y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos del Ministerio, deberán seguir con el procedimiento definido por la OTIC "Solicitud de Servicios de Red y creación de Cuentas de Usuario".
- Los equipos de cómputo personales de los colaboradores que se conecten a las redes de datos del MVCT deberán cumplir con los requisitos o controles para su autenticación y podrán realizar las tareas para las que se autorizaron.
- La OTIC deberá controlar los accesos a la red mediante:
    - Definición de las cantidades, tipos y características de las diferentes redes

  - Definición de los roles de acceso a servicios de los diferentes usuarios.
- No se podrá utilizar ningún tipo de utilitario para conexión remota a la red interna del Ministerio, únicamente se deberá utilizar el autorizado por la OTIC.

**A.5.16 Gestión de identidad**

- La OTIC deberá definir un procedimiento para la creación y la cancelación de usuarios en el 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 de aquellos colaboradores que no tengan ningún vínculo laboral con el Ministerio.

**A.5.17 Información de autenticación**

- Todo usuario que quiera acceder a servicios o información de la plataforma tecnológica del Ministerio, 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 vigiladas por el coordinador del Grupo de Apoyo Tecnológico de la OTIC.
- Todos los colaboradores y terceras partes deberán cumplir las condiciones de acceso y mantener confidenciales las contraseñas para preservar el no repudio.
- La OTIC deberá generar registros de auditoría con eventos relacionados de seguridad, considerando criterios 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 estos.
- El administrador de la plataforma tecnológica del Ministerio 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 OTIC deberá implementar mecanismos de doble factor de autenticación.
- 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.
- Los usuarios son responsables del uso de las contraseñas de acceso que se le asignen para la utilización de los equipos o servicios tecnológicos del Ministerio.
- Las mismas contraseñas no se deberán utilizar en distintos servicios y sistemas.
- Las contraseñas afectadas o comprometidas se deben cambiar inmediatamente después de la notificación o cualquier otra indicación de un compromiso.
- El cambio de contraseña solo podrá ser solicitada por el titular de la cuenta o su Jefe inmediato.
- Las contraseñas deberán:
    - Después de 3 (tres) intentos no exitosos de ingreso de la contraseña, el usuario deberá bloquearse inmediatamente y esperar un tiempo determinado para volver a intentar, o solicitar el desbloqueo en 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 OTIC.
- El administrador de la plataforma tecnológica del Ministerio garantizará que la administración de la plataforma se realice con estaciones de acceso privilegiado para cada administrador (PAW).

### A.5.18 Derechos de acceso

- El administrador de la plataforma tecnológica se encarga de asignar los accesos a plataformas, usuarios y segmentos de red según los procesos formales de autorización definidos por los dueños de los activos de información, que pueden evaluarse por la segunda y tercera línea de defensa según 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 por el 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 e implementada por la dependencia correspondiente.

- Los sistemas de información y/o aplicaciones, si requiere una cuenta de correo electrónico, se usarán cuentas de servicio y prohibirán el uso de cuentas personales.
- Los propietarios de los sistemas de información deberán monitorear los derechos de acceso de los usuarios. Si un colaborador cambia de rol o de trabajo, se deberá modificar o eliminar el acceso al sistema.
- 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 de red 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 pasar forzosamente 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 OTIC a través del proveedor de tecnología 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 OTIC.
- En función de la justificación del usuario para obtener acceso remoto, la OTIC debe determinar el tipo y nivel de acceso que se 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 por VPN:
    - Acceso general: Acceso a correo electrónico corporativo, internet y portal corporativo (intranet) sin aplicaciones.
    - Acceso particular: El mismo acceso general, más los permisos necesarios para ingresar a sistemas o aplicaciones que se justifique y autorice.

  - Acceso a administradores de sistemas: Acceso a los sistemas e infraestructura asignada según sus funciones.
- El acceso remoto justificado de terceros diferente al proveedor que administra la plataforma no estará permitido a menos que exista una legítima necesidad justificada para otorgarles el servicio. El usuario externo deberá cumplir con un procedimiento formal de autorización definido por la OTIC.
- Las aplicaciones o sistemas de información nuevos, que sean desarrollados al interior del Ministerio o por terceros, deberán cumplir con que la autenticación de los usuarios se realice a través del directorio activo.
- La OTIC deberá garantizar a través del administrador de la plataforma tecnológica la gestión de identidades.

**A.5.19 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.
- Los proveedores de Ministerio deberán identificar recurrentemente los riesgos de la seguridad de la información e informar al Ministerio los planes de tratamiento.
- Los proveedores deberán informar los controles técnicos, humanos y administrativos implementados para propender por confidencialidad, integridad y disponibilidad de la información del Ministerio.
- Los proveedores deberán tener acceso, monitoreo, control y/o gestionar la información, los servicios TIC, y la infraestructura física que sea necesaria para el cumplimiento de sus obligaciones contractuales.
- La Oficina de contratos deberá incluir cláusulas de confidencialidad, cumplimiento de políticas del SIG y derechos de propiedad intelectual en cada proceso contractual que se adelante desde el Ministerio.
- Todos los proveedores deberán realizar, al finalizar el contrato, la entrega de todos los activos de información que hubieren estado bajo su custodia.
- El Ministerio podrá realizar evaluaciones de los controles de la seguridad de la información que este en custodia de terceros o proveedores.
- Los proveedores deberán tener medidas de recuperación y contingencia para asegurar la disponibilidad de la información del Ministerio, y el procesamiento de esta.

**A.5.20 Abordar la seguridad de la información en los acuerdos con los proveedores**

- Todas las dependencias deberán establecer en los contratos con terceros y proveedores, cuando aplique, los requisitos legales y regulatorios

relacionados con la protección de datos personales, los derechos de propiedad intelectual y derechos de autor, así como requisitos de seguridad de la información, tales como:
    - Identificación de la información que se proporcionará o se le permitirá el acceso.
    - Métodos por los cuales se proporciona o se permitirá acceder a la información.
    - Identificación de la clasificación de la información que se proporcionará o se le permitirá el acceso.
    - Se deben definir por parte del Ministerio y por parte del tercero controles de acceso, la revisión del desempeño, uso aceptable de los activos, el monitoreo, informes auditoria entre otros, los cuales son de obligatorio cumplimiento por parte del tercero.
    - Se deben establecer acuerdos de nivel de servicio o planes de contingencia para los servicios en los que pueda aplicar.
- Todas las dependencias que compartan información con un tercero o proveedor deberán establecer métodos y procedimientos para dejar de compartir la información.
- La OTIC deberá documentar, establecer controles y permisos cuando un tercero o proveedor requiera tener accesos a la información por medio de la infraestructura tecnológica del Ministerio.
- La OTIC 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 se relacione con proveedores y su cadena de suministro, solicitará capacitación periódica a la OTIC sobre seguridad de la información para conocer las políticas del Ministerio.
- Un funcionario del Ministerio autorizará a todos los proveedores, usuarios externos y funcionarios de entidades externas, responsable de controlar y vigilar el uso adecuado de la información y los recursos de TI institucionales.
- Es responsabilidad de los terceros dar a conocer al ministerio cuando se presente un incidente de tecnología o de seguridad de la información, de igual manera colaborar en la contención, investigación y solución de este.
- Es responsabilidad de los terceros en caso de subcontratación dar a conocer los lineamientos de seguridad de la información definidos por el Ministerio.
- EL Ministerio podrá auditar los procesos contratados para validar que los lineamientos de seguridad de la información cumplan.
- Es responsabilidad de los terceros entregar informes del cumplimiento de

los controles de seguridad cuando el supervisor del contrato lo requiera.
- Las dependencias del Ministerio, que manejen información clasificada como reservada, deberán establecer controles de seguridad de la información definidos por el dueño o responsable de la misma.

**A.5.21 Gestión de la seguridad de la información en la cadena de suministro de tecnologías de la información y la comunicación (TIC)**

- La OTIC y el oficial de seguridad deberán definir los requisitos de seguridad que se aplicarán cuando se adquiera un producto o servicio de tecnología.
- Los terceros deberán garantizar que los requisitos de seguridad definidos por el MVCT se propaguen a lo largo de la cadena de suministro.
- Es responsabilidad de los terceros dar a conocer al Ministerio toda la información acerca de los componentes de software utilizados en los productos entregados a la entidad.

**A.5.22 Seguimiento, revisión y gestión de cambios de servicios de proveedores**

- Los proveedores y usuarios externos deben mantener y mejorar las políticas, los procedimientos y los controles de seguridad de la información existentes para gestionar cualquier cambio en la prestación de servicios por parte de los proveedores.
- Cada dependencia deberá evaluar periódicamente que los proveedores mantienen niveles adecuados de seguridad de la información.
- Los proveedores deberán proporcionar información a la dependencia, y está a la OTIC, sobre incidentes de seguridad de la información, y la OTIC deberá revisar esta información de acuerdo con los acuerdos establecidos y cualquier guía o procedimiento de apoyo.
    - Las responsabilidades de la OTIC y los proveedores asignados incluyen revisar las pistas de auditoría y registros de eventos de seguridad de la información, así como, problemas operativos, fallas y rastreo de fallas relacionadas con el servicio. También se debe responder y gestionar cualquier evento o incidente de seguridad identificado, identificar y gestionar vulnerabilidades de seguridad, y revisar los aspectos de seguridad de la información en las relaciones del proveedor con sus propios proveedores.
    - Cada dependencia debe monitorear, revisar y gestionar los cambios en las prácticas de seguridad y los estándares de prestación de servicios de un proveedor.
    - Cada dependencia, según aplique, deberá realizar, de manera continua o periódica, procesos de gestión de la relación con los proveedores, lo cual implica:

- Supervisar el desempeño del servicio para garantizar el cumplimiento de los acuerdos.
- Gestionar los cambios realizados por los proveedores, que abarcan desde mejoras en los servicios actuales hasta el desarrollo de nuevas aplicaciones y sistemas, pasando por ajustes en políticas y procedimientos, así como controles adicionales para abordar incidentes de seguridad de la información y mejorar la seguridad en general.
- Vigilar los cambios en los servicios del proveedor, incluyendo modificaciones en redes, la adopción de nuevas tecnologías, la incorporación de nuevos productos o versiones, la introducción de herramientas y entornos de desarrollo, cambios en la ubicación física de las instalaciones de servicio, la elección de subproveedores y decisiones de subcontratación a otros proveedores.

- La OTIC tiene la responsabilidad de asegurar que los proveedores de tecnología cuenten con suficiente capacidad de servicio y planes viables para mantener los niveles acordados de continuidad del servicio después de fallas importantes o desastres.

### A.5.23 Seguridad de la información para el uso de servicios en la nube

Los procesos de adquisición, uso, gestión y salida de los servicios en la nube se deben establecer de acuerdo con los requisitos de seguridad de la información de la organización. El Ministerio a través de la OTIC deberá llevar a cabo las siguientes acciones para mantener la seguridad de la información y el uso de servicios en la nube:

- Definir los requisitos de seguridad de la información en la nube,
- Definir los criterios de selección y alcance del uso de los servicios en la nube,
- Definir las funciones y responsabilidades relacionadas con su uso y gestión,
- Definir los controles de seguridad gestionados por el Ministerio y el proveedor,
- Definir el uso de capacidades de seguridad proporcionadas por el proveedor,
- Obtener garantías sobre los controles implementados por el proveedor,
- Administrar múltiples servicios en la nube,
- Manejar incidentes de seguridad en la nube,

- Monitorear y evaluar el uso continuo, y
- Establecer estrategias de cambio o terminación del uso de los servicios en la nube.
- Los procesos de adquisición, migración, uso, gestión y cancelación de los servicios en la nube se establecerán de acuerdo con el Análisis de Riesgo apropiado, los objetivos misionales y funcionales del Ministerio, y la estrategia indicada por la OTIC mediante el formato de Control de Cambios, para el apoyo y realización de dichas actividades.
- Un acuerdo entre el Ministerio y el proveedor de servicios en la nube debe incluir las siguientes disposiciones:
- Proporcionar soluciones basadas en estándares aceptados por la industria para la arquitectura y la infraestructura de servicios en la nube.
- Administrar los controles de acceso del servicio en la nube para cumplir con los requisitos del Ministerio.
- Implementar soluciones de protección y monitoreo de malware;
- Procesar y almacenar la información confidencial del MVCT en ubicaciones aprobadas o dentro o sujeto a una jurisdicción en particular;
- Brindar soporte dedicado en caso de un incidente de seguridad de la información en el entorno del servicio en la nube;
- Garantizar que se cumplan los requisitos de seguridad de la información del Ministerio en caso de que se subcontraten servicios en la nube a un proveedor externo
- Apoyar al Ministerio en la recopilación de evidencia digital, teniendo en cuenta las leyes y regulaciones sobre evidencia digital en Colombia.
- Proporcionar soporte y disponibilidad de los servicios durante un período de tiempo apropiado en caso de que el Ministerio decida cancelar los servicios en la nube.
- Proporcionar la(s) copia(s) de seguridad necesaria(s) de los datos y la información de configuración y gestionar de forma segura las copias de seguridad, según corresponda, en función de las capacidades del proveedor de servicios en la nube utilizado por la organización, actuando como cliente del servicio en la nube; Proporcionar la(s) copia(s) de seguridad necesaria(s) de los datos y la información de configuración y gestionar de forma segura la(s) copia(s) de seguridad, según corresponda, en función de las capacidades del proveedor de servicios en la nube utilizado por el Ministerio.

  - Proporcionar y devolver información como archivos de configuración, código fuente y datos que son propiedad del Ministerio, actuando como cliente del Ministerio, cuando se solicite durante la prestación del servicio o al finalizar el servicio.
- El Ministerio exigirá a los proveedores de servicios en la nube que proporcionen una notificación previa antes de que se realicen cambios sustanciales que afecten al Ministerio en la forma en que se entrega el servicio a la organización, incluidos:
  - Cambios en la infraestructura técnica que afecten o modifiquen la oferta de servicios en la nube;
  - procesar o almacenar información en una nueva jurisdicción geográfica o legal;

**A.5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información.**

- El Ministerio deberá planificar y prepararse para la gestión de incidentes de seguridad de la información definiendo, estableciendo y comunicando procesos, roles y responsabilidades de gestión de incidentes de seguridad de la información.
- La OTIC deberá definir los lineamientos para:
  - Responsables de la gestión de incidentes de seguridad de la información.
  - Los canales para que los colaboradores del Ministerio 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 OTIC 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 OTIC deberá proporcionar los medios para el aprendizaje al Ministerio de los incidentes de seguridad de la información.
- La OTIC deberá dar a conocer a los colaboradores del Ministerio, los lineamientos establecidos para la gestión de incidentes de seguridad de la información.
- Los proveedores de bienes y/o servicios deberán dar cumplimiento al procedimiento definido y adoptado por Ministerio para la gestión de incidentes.

## A.5.25 Evaluación y decisión sobre eventos de seguridad de la información.

Ministerio de Vivienda, Ciudad y Territorio deberá evaluar los eventos de seguridad de la información y decidir si se clasificarán como incidentes de seguridad de la información. Para tal efecto, se deberá acudir a los conceptos dados como evento e incidente, definidos en el presente manual.

- Los siguientes son 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.

## A.5.26 Respuesta a incidentes de seguridad de la información.

- La OTIC definirá los canales por medio de los cuales los Servidores Públicos, contratistas y terceros del Ministerio pueden reportar los incidentes de Seguridad o vulnerabilidad de la Información.
- 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 partes involucradas en el incidente, estén informadas.
- Todos los incidentes de seguridad serán 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.
- El proveedor de Tecnología será la encargada de recolectar las evidencias de los incidentes o vulnerabilidad de seguridad de la información.
- El proveedor de Tecnología deberá documentar y comunicar los incidentes o vulnerabilidad de seguridad de la información para el aprendizaje del Ministerio.
- El proveedor de Tecnología deberá asegurar que la recolección de evidencia

tenga en cuenta la cadena de custodia, la seguridad del personal, los roles y responsabilidades del personal involucrado, la competencia del personal, y la documentación.

**A.5.27 Aprender de los incidentes de seguridad de la información**

- La OTIC a través del Proveedor de Tecnología deberán realizar análisis de vulnerabilidades a la plataforma tecnológica de la entidad que permita establecer el plan de remediación, con el fin de cerrar las brechas de seguridad que sean encontradas.
- El Proveedor deberá realizar análisis forense informático, en caso de que se produzcan incidentes de seguridad de la información que requieran investigación.
- La OTIC deberá crear bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones, para reducir el tiempo de respuesta para los incidentes futuros.
- El procedimiento de gestión de incidentes de seguridad de la información deberá definir las actividades específicas para el reporte de los incidentes de seguridad o vulnerabilidad de la Información, valoración y soluciones ante incidentes de seguridad de la información, conocimiento y compendio de evidencias asociadas a los incidentes de seguridad de la información.

**A.5.28 Recolección de evidencia**

- La OTIC tendrá la responsabilidad de establecer bases de datos de incidentes junto con sus soluciones correspondientes. La iniciativa pretende agilizar los tiempos de respuesta ante incidentes futuros.
- El Oficial de Seguridad de la Información debe definir e implementar procedimientos para la identificación, recopilación, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información. Según los diferentes medios de almacenamiento, dispositivos y estado de los dispositivos (encendidos o apagados). Si no hay herramientas, se notificará a las autoridades competentes para realizar dicho procedimiento.
- La OTIC debe propender porque todos los sistemas de información tienen tablas de auditoría, donde la gestión directa de la información registra eventos como: modificación, borrado, creación, asignación de roles y privilegios, entre otros. Estos eventos los definirá el propietario de la información y la OTIC.
- La OTIC, debe conservar los eventos de auditoría de los sistemas de información y/o aplicaciones de acuerdo con lo establecido en las tablas de retención documental del proceso (medio y tiempo).
- Los dueños de los activos de información física deben conservar la evidencia

de préstamo de esta de acuerdo con las tablas de retención documental.

- Para la resolución de incidentes de seguridad de la información es necesaria la recolección de evidencia. Estas evidencias pueden provenir de diferentes fuentes, tales como:

    - Información basada en la red: Logs de IDS o IPS, logs de monitoreo, logs de routers, logs de firewalls, información recolectada mediante Sniffers de red, información de servidores de autenticación.
    - Información Basada en el Equipo: Live data collection: Volcado (dump) de la memoria RAM, fecha y hora del sistema, procesos activos, conexiones de red establecidas, puertos abiertos, aplicaciones escuchando en dichos puertos, estado de la tarjeta de red.
    - Otra información: Testimonio de funcionario, contratista o tercero que reporta el evento.

- En caso de que se requiera hacer denuncias penales, se debe tener en cuenta el Directorio Contacto con Autoridades y Grupos de Interés. Adicionalmente, es importante hacer una recolección y manejo adecuado de la evidencia; para ello, la entidad puede contactar al ColCERT, contratar un experto en el tema. En caso de que se tipifique como un posible delito se debe contactar a las autoridades competentes quienes realizarán la recolección de evidencia.
- La OTIC con apoyo del proveedor de tecnología deberá recolectar la evidencia digital de los incidentes que se presenten en la plataforma tecnológica.

## A.5.29 Seguridad de la información durante la interrupción

- La OTIC 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 OTIC con el apoyo del proveedor de tecnología deberán diseñar estrategias de recuperación de los servicios críticos de tecnología, contemplando los lineamientos de la seguridad de la información.
- Cada servicio tecnológico identificado como critico o esencial deberá contar con planes de contingencia.

## A.5.30 Preparación de las TIC para la continuidad del negocio.

- Se establecerán medidas y procedimientos para garantizar que el Ministerio

esté preparado y disponible en caso de interrupciones o desastres que puedan afectar los activos críticos, el cumplimiento de los objetivos misionales, la confidencialidad, la integridad o la disponibilidad de la información. Esto incluye la implementación de planes de continuidad del negocio, respaldo y recuperación de datos, y la realización de pruebas periódicas para asegurar la efectividad de las medidas implementadas. Además, de identificar los activos de información críticos, establecerán medidas de protección adecuadas para asegurar su disponibilidad y recuperación en situaciones adversas.

- La OTIC deberá diseñar una herramienta para analizar el impacto del negocio tecnológico del ministerio, identificando los servicios críticos tecnológicos del Ministerio.
- La OTIC 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 proveedor de servicios en acompañamiento de la OTIC deberá definir el plan de recuperación tecnológica y los planes de contingencia de los servicios de tecnología deberán se probados como mínimo una vez al año.
- 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.
- GAUA deberá definir estrategias de continuidad de la información física del MVCT.
- La OTIC deberá revisar y aprobar todos los planes de continuidad de negocio asociados con tecnología.

## A.5.31 Requisitos legales, estatutarios, reglamentarios y contractuales.

- La OTIC deberá identificar, documentar y actualizar la legislación referente a seguridad de la información en el normograma de la OTIC.
- Los propietarios de los activos los responsables de la clasificación de la información, al igual que establece controles para el acceso a la misma, teniendo en cuenta la normatividad vigente.
- Los funcionarios y contratistas deberán conocer las restricciones al tratamiento de los datos y de la información respecto a la que acceden por el 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.
- Con este instrumento el subscriptor se comprometerá a utilizar la información solo para su uso específico y a no comunicar, diseminar o de cualquier 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.
- La OTIC o los propietarios de los activos deberán analizar si deben ajustar controles de acuerdo con la normatividad vigente.
- Los propietarios de los activos son los responsables de la identificación de los riesgos asociados a los activos identificados en los procesos. La OTIC podrá brindar acompañamiento a los procesos en esta actividad.
- Todos los contratos del Ministerio deberán estipular cláusulas de seguridad de la información o del cumplimiento de las directrices definidas en el manual de seguridad y privacidad de la entidad.

## A.5.32 Derechos de propiedad intelectual

- La OTIC deberá definir controles para proteger adecuadamente la propiedad intelectual propia y de terceros, como derechos de autor de software, licencias y código fuente.
- La OTIC deberá generar conciencia a los colaboradores del Ministerio 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.
- 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 Ministerio, que se desarrollen de manera

colectiva y/o individual, bajo las políticas y directrices institucionales, son propiedad del Ministerio, 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 Ministerio.

En consecuencia, los funcionarios y contratistas están obligados a poner en conocimiento de sus jefes tales elementos de desarrollo, realizado con recursos del Ministerio y a transferir solemnemente, cuando por ley se requiera, todos los derechos derivados de estos a favor del Ministerio.

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

Con este propósito, los contratos escritos entre los desarrolladores del software y el Ministerio deberán incluir cláusulas explícitas que establezcan:

- La remuneración pactada
- Que todos los desarrollos de software se elaboran por cuenta y riesgo del Ministerio.
- Que todos los desarrollos de software serán de propiedad del Ministerio y este conservará todos los derechos patrimoniales sobre estos desarrollos.
- El plan señalado por el Ministerio determinando condiciones de necesidad, características y atributos de la obra, y estableciendo los lineamientos de tiempo, modo y lugar para su desarrollo.

### A.5.33 Protección de registros

- El Grupo de Atención al Usuario y Archivo (GAUA) y la OTIC deberán definir y establecer:
  - Directrices sobre retención, clasificación, almacenamiento, cadena de custodia, 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, manipulación de los registros e información física y digital, y tiempo de conservación de estos.

**A.5.34 Privacidad y protección de la información de identificación personal (PII)**

- El Ministerio deberá tomar las precauciones para conservar la confidencialidad y la integridad de los datos personales que la entidad conserve de funcionarios, contratistas o terceros, almacenados o archivados en cualquier medio, entre otros: información numérica, alfabética, gráfica, fotográfica, audiovisual o de cualquier otro tipo de 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.
- La oficina de encargada del manejo de datos personales del MVCT es la responsable de definir los controles del buen uso de esta.

**A.5.35 Revisión independiente de la seguridad de la información.**

- La OTIC, 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 (OCI) realizará evaluaciones independientes basadas en las muestras de los sistemas de información y al SGSI del Ministerio, con un enfoque en riesgos de seguridad digital, de acuerdo con 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.
- Además de las revisiones independientes periódicas, es importante considerar realizar revisiones independientes en situaciones como:
    - cambios en leyes y regulaciones,
    - incidentes significativos,
    - la introducción de nuevos procesos o modificaciones en los procesos existentes,
    - modificaciones sustanciales en los controles y procedimientos de seguridad de la información dentro del Ministerio.

**A.5.36 Cumplimiento de políticas, normas y estándares 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 (SIG).
- Si se encuentra algún incumplimiento, los lideres de los procesos deben:
  - identificar las causas del incumplimiento;
  - evaluar la necesidad de acciones correctivas para lograr el cumplimiento;
  - implementar acciones correctivas apropiadas;
  - revisar las acciones correctivas tomadas para verificar su efectividad e identificar cualquier deficiencia o debilidad.

### A.5.37 Procedimientos operativos documentados

- La OTIC deberá documentar y mantener actualizados todos sus procedimientos operativos del Ministerio asociadas con la seguridad de la información, para garantizar la disponibilidad, integridad y confidencialidad de la información.
- La OTIC deberá poner a disposición de todos los colaboradores los procedimientos de operación de los sistemas de información, los cuales deben especificar:
  - las personas responsables;
  - la instalación y configuración segura del sistema;
  - procesamiento y manejo de información, tanto automatizado como manual;
  - copia de seguridad y resiliencia;
  - requisitos de programación, incluidas las interdependencias con otros sistemas;
  - instrucciones para el manejo de errores;
  - contactos de soporte y escalamiento;
  - instrucciones de manejo de medios de almacenamiento;
  - procedimientos de reinicio y recuperación del sistema;
  - procedimientos de seguimiento inmediato tales como cambios en

configuración, capacidad, desempeño y seguridad;
- instrucciones de mantenimiento.

- Todo equipo de TI debe ser revisado, registrado y aprobado por la OTIC antes de conectarse a cualquier punto de la red de comunicaciones y datos del Ministerio, aquellos dispositivos que no estén aprobados y reportados tal conexión como un evento de seguridad deberán estar desconectados.

## A.6 CONTROLES DE PERSONAS

### A.6.1 Investigación de Antecedentes

Ministerio de vivienda, ciudad y territorio, garantizara por medio de un procedimiento definido y adoptado, que se realizara la verificación de antecedentes de todos los candidatos para convertirse en personal, la aplicación de dicho procedimiento deberá llevarse a cabo antes de unirse a la organización y de manera continua, teniendo en cuenta las leyes, los reglamentos y la ética aplicables, y serán proporcionales a los requisitos comerciales, la clasificación de la información a la que se accederá y los riesgos percibidos.

- 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 Ministerio 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 documentos de verificación deberán reposar en la historia laboral o carpeta contractual del colaborador. Se deberá definir el medio (físico y/o digital) y la estructura de organización de esos documentos y los privilegios que se puedan otorgar al personal correspondiente para consultarlo.
- 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.6.2 Términos y condiciones de empleo

- Los contratos de trabajo que se perfeccionen en el Ministerio deben dejar definidas claramente las responsabilidades del personal y de la organización en materia de seguridad de la información.
- 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 Ministerio.

- El Grupo de Talento Humano y el Grupo de Contratos deberán firmar un documento de confidencialidad de la información que contenga como mínimo el cumplimiento de las políticas institucionales y normatividad vigente a los funcionarios del Ministerio, cualquiera sea su situación contractual, la dependencia y las tareas que desempeñe, dicho documento debe reposar en la historia laboral o expediente contractual según el caso.

### A.6.3 Concientización, educación y capacitación en seguridad de la información.

El personal de Ministerio de Vivienda, Ciudad y Territorio y las partes interesadas relevantes deben recibir la conciencia, educación y capacitación adecuadas en seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, las políticas y los procedimientos específicos del tema, según sea relevante para su función laboral.

- En la inducción y capacitación del cargo a personal vinculado al Ministerio de Vivienda, Ciudad y Territorio, deberá definirse un espacio de tiempo puntual para concienciar, eduque y capacitar en la política de seguridad de la información definida y adoptada en la entidad mediante el Manual de Seguridad y Privacidad de la Información.
- El equipo de seguridad de la información deberá definir en cada vigencia un plan de sensibilización en seguridad de la información que incluya actividades mensuales y actores que harán parte de ella; también canales físicos o virtuales adecuados, como campañas, folletos, carteles, boletines, sitios web, sesiones informativas, módulos de aprendizaje y correos electrónicos.

### A.6.4 Proceso Disciplinario.

- El Ministerio formalizará y comunicará un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información.

- El incumplimiento de las políticas de seguridad de la información del Ministerio 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 Ministerio y los acuerdos firmados por los funcionarios.
- Con la implementación de políticas en seguridad de la información, el Ministerio cumple las disposiciones legales y regulatorias emitidas por los organismos estatales, para tener una metodología de gestión de riesgos como herramienta para actuar proactivamente ante situaciones que puedan afectar la continuidad de los procesos del Ministerio.
- Todos los colaboradores del Ministerio (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.

### A.6.5 Responsabilidades después de la terminación o cambio de empleo.

- El supervisor del contrato o a quien delegue deberá custodiar la información del Ministerio 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 Ministerio bajo la responsabilidad de los funcionarios públicos 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 OTIC a través del canal dispuesto para este fin, cualquier novedad de desvinculación administrativa, laboral, contractual o cambio de rol del servidor público, colaborador o tercero. Una vez notificada la novedad la OTIC deberá proceder a la inactivación de los accesos y servicios de red, 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.
    - Si el buzón es investigado por las autoridades competentes, se les entregará en cadena de custodia una copia garantizando su integridad.
    - Emitir comunicado a los proveedores y demás personal con el que el funcionario público o colaborador tenga contacto, indicándole que

esa persona ya no labora en el Ministerio e indicar quién asumirá sus funciones o responsabilidades.
    - El buzón de correo electrónico del funcionario público, colaborador o tercero 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 funcionario público o colaborador del Ministerio.
- 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 los activos de información según lo determina el procedimiento de terminación del empleo, el proceso de entrega del cargo o separación temporal del mismo y los informes de supervisión de contrato según 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.6.6 Acuerdos de confidencialidad o no divulgación

Los contratistas, funcionarios o terceros que por diferentes razones requieran conocer o intercambiar información clasificada y reservada se obligan para con el MVCT a no revelar, divulgar, exhibir, mostrar, comunicar, utilizar y/o emplear la información, por él conocida en desarrollo de sus funciones u obligaciones, en su favor o en el de terceros y en consecuencia a mantenerla de manera confidencial y privada, evitando cualquier tipo de reproducción o de uso indebido de los datos.

- La información conocida por los contratistas, funcionarios o terceros sólo podrá ser utilizada para desarrollar las funciones o actividades propias del objeto contractual.
- El grupo de contratos debe incluir en los acuerdos con proveedores y contratistas una cláusula que defina las responsabilidades que continúan después de terminado el contrato según sea el caso
- 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 Ministerio, 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 Ministerio, 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 los contratistas y proveedores, los contratos deben incluir una cláusula de confidencialidad, igual que si se permite el acceso a la información y/o a los recursos del MVCT a personas 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 esta y los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad, disponibilidad y requerimientos.
- Los acuerdos de confidencialidad deben aceptarse por contratistas y proveedores como parte del proceso de contratación, razón por la que dicha cláusula y/o acuerdo de confidencialidad forman parte integral de cada contrato.
- El incumplimiento de los acuerdos de confidencialidad acarreará las consecuencias contractualmente previstas y las acciones disciplinarias necesarias.

### A.6.7 Trabajo a distancia

- Los criterios y condiciones para ejercer la modalidad de teletrabajo o trabajo remoto los definirá el comité de Teletrabajo, con base en la normativa legal vigente mediante la formalización y/o actualización de procedimientos que incluyan los aspectos de seguridad de la información.
  - Teletrabajo: Está regulado por la Ley 1221 de 2008, el Decreto 884 de 2012, la Circular 021 de 2020, la Resolución 2886 de 2012, el Decreto 1227 de 2022 y la Resolución 3192 de 2022.
  - Trabajo en casa: Está contemplado en la Ley 2088 de 2021 y el Decreto 649 de 2022.
  - Trabajo remoto: Regulado por la Ley 2121 de 2021 y el Decreto 555 de

2022.

- Los colaboradores que requieran acceder a los recursos informáticos del MVCT fuera de las instalaciones de este 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 OTIC.
- Las conexiones de la modalidad de teletrabajo o trabajo remoto deberán ser monitoreadas y supervisadas según el perfil de usuario y/o asignación de roles y privilegios, igualmente verificar la desactivación de los accesos una vez el funcionario o contratista no tenga vinculación con la entidad.
- Antes de aprobarse, el acceso a servicios de teletrabajo debe evaluarse riesgos de seguridad de la información y 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 OTIC 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 OTIC.
- 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 pronto la posible pérdida o hurto de los equipos y/o dispositivos móviles usados para teletrabajo o el trabajo remoto y que estén 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 OTIC 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 OTIC, para que le sean modificados los accesos concedidos.

### A.6.8 Reporte de eventos de seguridad de la información

- Los funcionarios, contratistas, proveedores o terceros y quien tenga acceso a la información del MVCT debe reportar los eventos de seguridad de la información identificados, según el Proceso Gestión de Incidentes de Seguridad.
- Todos los funcionarios, colaboradores o terceros deberán reportar a través de los canales definidos cualquier situación que se pueda considerar como un evento de seguridad de la información.
- La OTIC a través del proveedor de tecnología debe identificar las diferentes situaciones que están involucradas en el incidente como un incumplimiento a la integridad, disponibilidad o confidencialidad, control de seguridad insuficiente o ineficaz, errores humanos, vulneración de seguridad física, negación de acceso, mal funcionamiento del software, cambios no controlados, etc.
- Es responsabilidad de todos los colaboradores, funcionarios y contratistas, del MVCT reportar oportunamente cualquier posible vulneración de seguridad de la información o incidente relacionado con los recursos informáticos. Este reporte debe realizarse a través del Jefe de la dependencia al Líder del Sistema de Gestión de Seguridad de la Información, quien en colaboración con el Jefe de la OTIC facilitaran las herramientas informáticas necesarias y garantizaran que los informes se formalicen de manera adecuada y en el menor tiempo posible.
- Toda falla aparente de cualquier sistema de información o software debe reportarse a la OTIC, si es un sistema de información adquirido a terceros,

debe reportarse la falla al proveedor del software.

- Todo reporte de incidentes debe ser detallado posible, incluyendo la mayor cantidad de evidencias que agilicen la gestión de este. Además, los colaboradores tienen la opción de mantener el anonimato al realizar su reporte o denuncia, si así lo desean.
- Todos los reportes se manejarán 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.
- 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.
- Cualquier intento de interferencia, obstrucción o de disuadir a quien reporta una posible vulneración 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.
- 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.
- El MVCT a través de la OTIC 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.

## A.7 CONTROLES INFRAESTRUCTURA FISICA

### A.7.1 Perímetros físicos de seguridad

- La Oficina de recursos físicos con acompañamiento de la OTIC, deberán definir las áreas seguras del MVCT.
- El perímetro de las áreas que contienen la información y sus instalaciones de procesamiento sensible o critico deberán estar protegidos de accesos no permitidos.
- Las puertas y ventanas de las áreas seguras deberán permanecer cerradas con llave cuando no hay supervisión o están desocupadas.
- Las puertas y ventanas de las áreas seguras deberán permanecer cerradas con llave cuando no hay supervisión o están desocupadas.
- El proveedor de tecnología deberá establecer los controles necesarios para limitar el acceso al centro de datos.

- El Grupo de Recursos Físicos, deberá monitorear y probar todas las puertas contra incendios o salidas de emergencia con el fin de propender por el correcto funcionamiento.

### A.7.2 Entrada física

- Todos los puntos de acceso deberán tener un área de recepción con vigilancia u otro medio para controlar el acceso físico al sitio o edificación.
- 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 de las instalaciones principales del Ministerio. Para garantizar el acceso solo al personal autorizado.
- 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 definir en cuales áreas seguras se debe implementar un registro de entrada y/o salida. Es responsabilidad del área dueña del área segura conservar los registros de ingreso o salida, de acuerdo con lo definido en las tablas de retención documental.
- Los respaldos de la información digital del CCTV, se deberá conservar por 60 días.
- El proveedor de tecnología deberá establecer los controles de ingreso, mecanismos de autenticación para el ingreso al centro de datos.
- Todos los colaboradores del MVCT, deberán portar en un lugar visible el carné de identificación mientras se encuentren en las instalaciones de este.
- Todos los visitantes deben portar una escarapela o sticker de identificación mientras permanezcan en las instalaciones del MVCT.
- El Grupo de Recursos Físicos deberá revisar semestralmente los accesos de los colaboradores a las áreas seguras y ajustarlos en caso de ser necesario.
- El Grupo de Recursos Físicos deberá implementar un sistema de registro de visitantes, consignado fecha y hora de ingreso y de salida, área a la cual se dirige.

### A.7.3 Asegurar oficinas, salas e instalaciones

- 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 Ministerio equipos fotográficos, de video, audio u otro equipo de grabación, como cámaras en dispositivos móviles, salvo autorización para ello del área encargada. CCTV monitorea el trabajo en áreas seguras, considerando 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.7.4 Monitoreo de seguridad física

- Para proteger los activos de información y salvaguardar las instalaciones del MVCT, el Grupo de Recursos Físicos establecerá medidas de monitoreo de seguridad física para detectar y responder oportunamente a cualquier incidente o actividad sospechosa. Esto incluye la instalación y configuración de sistemas de vigilancia, como cámaras de seguridad (CCTV) y sistemas de control de acceso, que permitan la supervisión continua de las instalaciones de las sedes. Además, se establecerán procedimientos para el seguimiento y análisis de los registros y eventos de seguridad física, con el objetivo de identificar posibles vulnerabilidades y mejorar las medidas de seguridad.
- 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 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 deberá definir y mantener un mapa de calor de las zonas protegidas de cada una de las sedes del Ministerio.

### A.7.5 Protección contra amenazas físicas y ambientales.

- El Grupo de Recursos Físicos debe realizar un análisis de riesgos de las amenazas físicas y ambientales con el fin de identificar los controles necesarios para minimizar su impacto o evitar su materialización.
- El Grupo de Recursos Físicos, para garantizar la protección de las áreas seguras físicas del MVCT contra amenazas físicas y ambientales, deberá implementar y administrar Sistemas de seguridad electrónica:
    - Circuito Cerrado de Televisión (CCTV)
    - Control de Acceso
    - Incendio: detección, alarma y extinción.
    - Detectores: de movimiento, sísmicos, de roturas de cristales, de presencia de monóxido de carbono.
    - Alarma: sirenas y botones de emergencia.
    - Comunicaciones con Centrales de Recepción de Alarmas.

### A.7.6 Trabajar en áreas seguras

- 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.
- El Grupo de Recursos Físicos deberá colocar controles de acceso para proteger la información y los activos en áreas públicas o compartidas.
- El GAUA deberá establecer políticas y procedimientos para el manejo y la protección de la información en áreas seguras físicas.
- La OTIC deberá establecer políticas y procedimientos para el manejo y la protección de la información en áreas seguras lógicas.
- Cada área responsable de información deberá capacitar al personal sobre las medidas de seguridad y el comportamiento adecuado en las áreas seguras físicas.
- La OTIC 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 OTIC 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 OTIC, 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 mantener libre de objetos o elementos que no sean propios en la operación en el centro de datos.

### A.7.7 Escritorio limpio y pantalla limpia

- La política de escritorio y pantalla despejados también están descritas en el numeral 12.2.6 POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIOS, del manual de Políticas.
- 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 en lugares físicos sin exposición 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.

### A.7.8 Ubicación y protección de equipos

- El Grupo de Recursos Físicos deberá establecer lineamientos para los controles de ubicación y protección de los equipos e impresoras teniendo en cuenta lo siguiente:
    - Se deberán ubicar y proteger para reducir el riesgo contra amenazas ambientales como incendios, inundaciones, terremotos, etc.
    - deberán estar protegidos por controles de acceso, para reducir el riesgo contra de acceso no autorizado, como cerraduras digítales, tarjetas de acceso, biometría, etc.
    - Se deberán implementar medidas para proteger los equipos contra robos, como el uso generalizado de guayas, sistemas de CCTV, sistemas de rastreo, controles de acceso biométrico a las áreas restringidas, evitar la presencia de personas no autorizadas sin escolta del personal de seguridad, etc.
    - Se deberán implementar medidas para proteger el equipo contra interferencias electromagnéticas que puedan afectar su funcionamiento.
    - Se prohíbe 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 efectuadaspor 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.
- Si se presenta una falla o problema de hardware o software en una estación de trabajo o equipo portátil propiedad del MVCT, el usuario responsable

deberá informarlo a la OTIC a través de la Mesa de Ayuda, para una asistencia especializada, y deberá intentar resolverlo.
- Las actividades de mantenimiento de los servidores, elementos de comunicaciones, energía o cualquiera que pueda ocasionar una suspensión en el servicio, deberán ser programadas.
- se deben implementar medidas de seguridad para proteger el equipo durante su transporte, como el uso de estuches o contenedores seguros, el cifrado de datos, etc.
- se deben implementar procedimientos seguros para la eliminación de equipos que ya no se utilizan, como el borrado seguro de datos, la destrucción física de discos duros, etc.

### A.7.9 Seguridad de los activos fuera de las instalaciones

- Los equipos de cómputo y portátiles que requieran salir de las instalaciones de MVCT para uso misional de los colaboradores deberán estar autorizados.
- Los equipos de red, computo, y portátiles que requieran salir de las instalaciones del MVCT para reparación o mantenimiento, deberán estar debidamente autorizados.
- El Grupo de Recursos Físicos se encargará de mantener un registro preciso en el almacén de los equipos, durante su asignación y durante su proceso de devolución.
- Todo equipo de cómputo, servidores o equipos activos de red propiedad del MVCT, que deban ser retirados de las instalaciones, deberán contar con:
    - La autorización del jefe de la OTIC.
    - El registro escrito del personal de seguridad.
- La OTIC deberá implementar las herramientas tecnológicas necesarias para el monitorio de los equipos de cómputo cuando se encuentren fuera de las instalaciones.

### A.7.10 Medios de almacenamiento

- Las áreas del MVCT que utilicen medios de almacenamiento deberán:
    - seleccionarlos y utilizarlos de acuerdo con las necesidades del MVCT y los requisitos de seguridad.
    - protegerlos contra daños, pérdida o acceso no autorizado.
    - almacenarlos en un lugar seguro y protegido.
    - etiquetarlos y registrarlos para mantener un control adecuado.
    - eliminarlos de forma segura cuando ya no sean necesarios.
- La OTIC debe definir políticas y controles para regular el uso de estos medios de almacenamiento. Por tanto, se restringe el uso de medios de almacenamiento removibles en la infraestructura de cómputo del MVCT, como CDs, DVDs, memorias flash, USBs, Ipods, celulares y cintas, a menos

que sea autorizado por la OTIC

- Los colaboradores autorizados a usar medios de almacenamiento removibles se deben comprometer a asegurar física y lógicamente el dispositivo para no arriesgar la información del MVCT que este contiene.
- En 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 de este.
- 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 OTIC 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 eliminarse, dar de baja o reasignarse deberán someterse a un proceso de borrado seguro y otros mecanismos considerados, para evitar la recuperación de la información que antes contenía 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 OTIC 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.7.11 Utilidades de apoyo/servicios de soporte/

- Las instalaciones de procesamiento de información dentro de los predios propios o en arriendo de MVCT deben protegerse contra cortes de energía y otras interrupciones causadas por fallas en los servicios públicos de apoyo.
- La OTIC 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 OTIC 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.
- Los cables de energía eléctrica deberán estar separados de los cables de comunicaciones para evitar interferencia.
- El Grupo de Recursos Físicos deberá planificar para cada anualidad, por lo menos, dos auditorías físicas en las instalaciones de red eléctrica y de transferencia de datos, para garantizar el cumplimiento de la norma definida.
- 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 OTIC deberá definir mecanismos de soporte y mantenimiento a los equipos.
- Deberá definirse un procedimiento para la ejecución de actividades de mantenimiento preventivo y correctivo que deban ser realizadas.
- Solo el personal autorizado deberá llevar a cabo el mantenimiento o las reparaciones a los equipos tecnológicos del MVCT.

### A.7.12 Seguridad del cableado

- Los cables que transportan energía, datos o servicios información de apoyo dentro de las instalaciones de MVCT deben estar protegidos contra

intercepciones, interferencias o daños.

- El cableado que transporta datos y suministro de energía deberán estar protegidos contra la interceptación, interferencia o daños.
- Debe definirse claramente los canales de ubicación física del cableado eléctrico y de red de manera que no se presente interferencia entre ellos.
- El Grupo de Recursos Físicos y la OTIC, deberán implementar controles que permitan hacer seguimiento a las variables de humedad y temperatura en los centros de cableado para garantizar condiciones operativas adecuadas.
- La OTIC 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 OTIC será responsable de mantener organizado e identificado el cableado en los racks de los centros cableado.
- El cableado debe tener identificación de origen y destino una vez sean instalados en la respectiva red.
- El Grupo de Recursos Físicos y la OTIC, 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 OTIC, 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 tiempoque 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.

### A.7.13 Mantenimiento de equipos

- Los equipos que hagan parte de la infraestructura del MVCT se mantendrán correctiva y preventivamente para garantizar la disponibilidad, integridad y confidencialidad de la información
- La OTIC deberá definir, documentar, implementar y hacer seguimiento de un procedimiento físico y lógico de mantenimiento para cada dispositivo que incorpore a la infraestructura tecnológica de la entidad.

- Los equipos críticos de comunicaciones deben ser alimentados por sistemas de potencia eléctrica regulados y estar protegidos por UPS.
- La OTIC 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 tienen prohibido 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, 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 estos.
- La protección física de las estaciones de trabajo, equipos portátiles y demás recursos informáticos corresponde a los responsables o custodios de estos y es su deber, notificar cualquier eventualidad que se presente sobre dichos equipos a la OTIC.
- 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 OTIC o, en su defecto, a su Jefe inmediato.
- El alistamiento de las estaciones de trabajo y equipos portátiles es responsabilidad de la OTIC, así como la eliminación segura de la información de estos.
- La OTIC debe procurar que todos los recursos informáticos como servidores, dispositivos de comunicación, estaciones de trabajo, equipos portátiles e impresoras, entre otros, propiedad del MVCT, estén continuamente

actualizados para conservar e incrementar la calidad del servicio que prestan, mejorando su desempeño y obteniendo mayor estabilidad y protección ante amenazas.

### A.7.14 Eliminación segura o reutilización de equipos

- Los elementos del equipo que contengan medios de almacenamiento se verificarán para garantizar que todos los datos confidenciales y el software con licencia se hayan eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.
- La OTIC deberá garantizar que cuando se retire un dispositivo de servicio, deberá eliminarse toda información mediante borrado seguro considerando que, previo a esta actividad, deberá resguardarse de esta.
- La OTIC deberá garantizar que, cuando se reasigne un dispositivo, este deberá formatearse e instalarse la línea base de software.

## A.8 CONTROLES TECNOLÓGICOS

### A.8.1 Dispositivos de punto final de usuario

Responsabilidad General

- La información clasificada como publica reservada o publica clasificada deberá almacenarse en los repositorios establecidos por la OTIC "OneDrive y servidores de archivo", no deberá guardarse en los discos duros del BYOD o en otros dispositivos personales.
- La OTIC, 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 conectados a las redes telecomunicaciones e infraestructura de tecnología de información y comunicaciones del MVCT.
- La autorización de la conexión de dispositivos 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 de los dispositivos (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 estos.
- En caso de pérdida o robo del dispositivo institucional el funcionario, contratista o tercero responsable de este, deberá comunicarlo inmediatamente a su jefe y debe reportar este hecho como un incidente de

seguridad a la OTIC a través de la Mesa de Ayuda y al Grupo de Recursos Físicos, para que sea atendido.

- La OTIC, deberá contar con una herramienta que permita hacer borrado seguro de la información del Ministerio en caso de pérdida o robo del dispositivo institucional.
- El Grupo de Recursos Físicos debe establecer un procedimiento ante pérdida de dispositivos 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).
- Para los dispositivos móviles propiedad del MVCT, la OTIC deberá disponer herramientas de ofimática, antivirus, medios de almacenamiento virtual (almacenamiento en nube), y las necesarias si son parte de la línea base de software del Ministerio, la restricción de software del usuario final de instalarlo.
- La OTIC debe sensibilizar a los propietarios o responsables de los dispositivos móviles sobre los cuidados y responsabilidades de cada componente 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.

Responsabilidad del Usuario

- Los colaboradores (funcionarios y/o contratistas) son responsables de la custodia de los dispositivos institucionales y se harán responsables dentro y fuera de las instalaciones de estos, por lo que deberá desarrollar mecanismos para respaldar información periódicamente, de requerir apoyo a la OTIC.
- 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 con un dispositivo móvil del MVCT se encargarán de usar bien la información del Ministerio almacenada en estos dispositivos

considerando que este 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.
-

Uso de dispositivos personales

- Los Líderes de procesos, jefes de Oficina y 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 procesar información institucional pública reservada o información pública clasificada, así como la aplicación de las políticas de seguridad requeridas para la información que se maneje en el dispositivo personal del funcionario, contratista o tercero.
- En ningún caso se autoriza almacenar información institucional en dispositivos que no pertenecen a la entidad (BYOD).
- Los Líderes de procesos deben evaluar los riesgos asociados a la divulgación de información pública reservada o información pública clasificada antes de autorizar el uso de dispositivos BYOD.
- La OTIC, mediante la mesa de servicio realizará 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 OTIC.
- Se debe mantener un registro y control formal de los dispositivos móviles autorizados a conectarse a las redes del MVCT.
- El funcionario, contratista o 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 que maneje en este será para uso exclusivo de sus funciones u obligaciones contractuales.
- Todo dispositivo BYOD autorizado para procesar información de la entidad debe cumplir con la reglamentación vigente en materia de uso de software legal. El usuario es responsable de contar con todo el software de su dispositivo licenciado.

- La OTIC, 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 maneje en el dispositivo personal.

### A.8.2 Derechos de acceso privilegiado

- El acceso a la información del MVCT se otorga solo a usuarios autorizados, considerando lo requerido para realizar 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.
- La OTIC deberá otorgar los privilegios para la administración de recursos tecnológicos, servicios de red y sistemas de información únicamente a aquellos colaboradores o terceros que cumplan dichas funciones.
- La OTIC deberá otorgar cuentas personalizadas con altos privilegios para cada administrador de recursos tecnológicos, servicios de red y sistemas de información, diferentes a los nativos y deberá ser única asociadas al usuario de dominio.
- La OTIC 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 OTIC deberá deshabilitar los servicios o funcionalidades no utilizadas de los sistemas operativos, el firmware y las bases de datos.
- La OTIC 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).
- 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.
- Se deben realizar revisiones de los privilegios de acceso a los sistemas de información, aplicaciones entre otras al menos una vez al año.
- Los funcionarios, contratistas y proveedores que tengan algún vínculo con el MVCT deberán hacerse responsables de los usuarios y contraseñas asignados para el acceso a los servicios que están en la red, los recursos de la plataforma tecnológica y los sistemas de información.

- Los funcionarios, contratistas y proveedores no podrán compartir sus cuentas de usuario y contraseñas con otros usuarios o con personas ajenas a la Entidad. Si esto llegara a pasar esto es causal de sanción por parte del Ministerio.
- 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 OTIC 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.

### A.8.3 Restricción de acceso a la información

- Todo funcionario del MVCT, cualquiera sea su situación contractual, su dependencia y el nivel de tareas debe tener asociado un perfil de uso de recursos de información, incluyendo el hardware y software asociado. La OTIC debe mantener un directorio completo y actualizado de tales perfiles.
- La OTIC 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 OTIC 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; implementar para los desarrolladores internos o externos acceso limitado y controlado a los datos y archivos de 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 forma segura, evitando indicar específicamente cuál fue la falla durante el proceso de autenticación y, en cambio, 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 usa la reasignación de contraseñas, solo se envíe un enlace o contraseñas temporales a cuentas de correo electrónico registradas en los aplicativos, que tendrán un periodo de validez establecido; se deberán forzar el cambio de las contraseñas temporales tras su uso.

### A.8.4 Acceso al código fuente

- Para acceder al código fuente se debe contar con autorización de la OTIC, lo anterior con el fin de evitar la introducción de funcionalidades no autorizadas, evitar cambios involuntarios y mantener la confidencialidad de propiedad intelectual.
- Para evitar la introducción de funciones no autorizadas, evitar cambios no intencionales o maliciosos y mantener la confidencialidad de la propiedad intelectual sobre el software, solo los ingenieros desarrolladores y de soporte autorizados por la OTIC, así como los propietarios de los activos de información, tienen la capacidad de acceder al código fuente del programa, las herramientas de desarrollo y las bibliotecas de software.
- Los desarrolladores deben proteger el código fuente de los aplicativos construidos, para que usuarios no autorizados no puedan descargarlo ni modificarlo.
- La OTIC debe establecer y mantener ambientes separados de Desarrollo/Pruebas y Producción, dentro de la infraestructura del MVCT, para evitar fraude o inserción de código malicioso.

### A.8.5 Autenticación segura

- La OTIC debe mantener continuo el directorio activo o al sistema empleado para la autenticación de usuarios para desactivar las cuentas de usuarios

que se desvincularon del Ministerio y verificar que las existentes corresponden a usuarios activos o vigentes del 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. Si existen excepciones, deberán ser justificadas y aprobadas.

- Las contraseñas de administrador de las aplicaciones o soluciones de software que producen procesan, gestionan o almacenan información crítica del Ministerio, deben conservarse por la OTIC:
    - debe existir una segregación de deberes y un protocolo que impidan que las contraseñas de administrador queden bajo la responsabilidad de una sola persona.
    - las contraseñas se deben cambiar en intervalos regulares de tiempo, máximo de 360 días y/o si el personal responsable cambia de cargo o de dependencia.
- La OTIC 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 sedeberá 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 OTIC 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.
- 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 OTIC.
- 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 deinformación que se tienen o administran en el Ministerio.

### A.8.6 Gestión de capacidad

- La OTIC deberá documentar la gestión de capacidad la cual le permita:
    - Evaluar las necesidades de capacidad de los sistemas en operación y proyectar las futurasdemandas 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.
    - Realizar pruebas de estrés de los sistemas para confirmar que hay suficiente capacidad.
    - Definir los indicadores de rendimiento correspondientes a la gestión de capacidad.
    - Deberá asignar un responsable de la gestión de capacidad.
- La OTIC 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 OTIC 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 OTIC 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 OTIC deberá generar reportes en cada solución, evidenciando que tipos de archivos están alojados, archivos por propietarios, duplicados, grandes, no usados recientemente, para determinar acciones que eviten fallas en la solución de almacenamiento del MVCT.
- El Grupo de Atención y Archivo deberá realizar la destrucción final de la información física que haya cumplido los tiempos de retención de acuerdo con las TRD.

### A.8.7 Protección contra Malware

- 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 OTIC deberá realizar campañas de concienciación a usuarios en materia de protección, prevención y recuperación contra códigos maliciosos.
- La OTIC deberá dictar los lineamientos para instalar software antivirus que proteja contra códigos maliciosos en los recursos informáticos del MVCT y asegurar que no puedan deshabilitarse estas herramientas y mantenerlas actualizadas permanentemente.
- La OTIC deberá implementar herramientas que recopilen datos, análisis de datos y detección y respuesta ante amenazas.

### A.8.8 Gestión de vulnerabilidades técnicas

- La OTIC y el proveedor de tecnología deberán actualizar continuamente el software de antivirus y actualizaciones de sistema operativo.
- Todo mensaje sospechoso de procedencia desconocida se reportará inmediatamente a la OTIC 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 OTIC, 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 OTIC.
- 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.
- La OTIC debe establecer un procedimiento asociado a las vulnerabilidades técnicas de la plataforma tecnológica de la entidad.
- La OTIC debe ejecutar análisis de vulnerabilidades planeados y documentados a la plataforma tecnológica de la entidad.
- La OTIC deberá proporcionar un mecanismo público de informe de vulnerabilidades de los servicios y/o aplicaciones institucionales.
- Las vulnerabilidades criticas o altas deben ser identificadas como riesgos digitales y se deben identificar en el proceso dueño de la información.
- Las remediciones sobre los análisis de vulnerabilidades se deben ejecutar a través del procedimiento de cambios.
- La OTIC deberá llevar una bitácora de las vulnerabilidades de la plataforma tecnológica.

### A.8.9 Gestión de la configuración

- Se implementarán procedimientos y controles que abarcan desde la adquisición y despliegue de nuevos activos hasta su mantenimiento y retirada, para garantizar que los activos de información tecnológicos del MVCT se encuentren correctamente configurados y sean consistentes con las políticas y estándares establecidos. Además, se establecerá un proceso de control de cambios para garantizar que cualquier modificación en la configuración sea aprobada, registrada y verificada antes de su implementación.
- La OTIC deberá implementar una herramienta que le permita hacer seguimiento al software y hardware de la plataforma tecnológica.
- La OTIC deberá realizar un inventario de los servicios tecnológicos que presta a la entidad.
- La OTIC y el proveedor de tecnología deberán administrar las plataformas a través de máquinas endurecidas (Privilege Adminstration Workstation - PAW).
- La OTIC deberá revisar semestralmente las cuentas de servicio y de usuario, para validar su uso en la plataforma. En caso de encontrarse cuentas de usuario o de servicio sin utilizar por más de noventa (90) días, estas deberán deshabilitarse.

- Los cambios en las configuraciones deberán seguir los procedimientos de Gestión de Cambios.

### A.8.10 Eliminación de información

- Se establecerán procedimientos y controles para asegurar la eliminación adecuada y segura de la información cuando ya no sea necesaria o cuando deba ser descartada, asegurando la trazabilidad y el cumplimiento de los requisitos aplicables: legales, estatutarios, reglamentarios y contractuales. Los procesos de eliminación deberán contar con las técnicas y herramientas adecuadas para garantizar que los datos sean completamente borrados o destruidos.
- La OTIC y el Grupo de Atención a usuarios y archivo deberán definir procedimientos para realizar la eliminación física y digital de la entidad.
- En caso de que la destrucción de la información la realice un tercero, se deberá solicitar un certificado de destrucción segura de la información.
- La destrucción de la información deberá cumplir con los requisitos legales establecidos y con los parámetros definidos en las TRD.
- La OTIC deberá solicitar al proveedor de nube el procedimiento de eliminación de la información de la entidad.

### A.8.11 Anonimización de datos

- El Oficial de Privacidad de la Información determinará los procesos de anonimización no reversibles que proporcionen versiones de datos anonimizados significativos y relevantes, que mantengan las propiedades estadísticas de los datos originales. Las versiones anonimizadas de datos deben cumplir con las disposiciones del Régimen General de Protección de Datos Personales (Ley 1581/2012 y Decreto 1317/2013). Estas versiones solo pueden utilizarse con fines legítimos, como análisis de datos, minería de datos, inteligencia de negocios, pruebas de software, capacitación de usuarios, entre otros, garantizando así el cumplimiento legal y normativo.

### A.8.12 Prevención de fuga de datos

- El MVCT deberá implementar tecnologías y políticas adecuadas para monitorear, detectar y prevenir la fuga de datos, tanto dentro del MVCT como en comunicaciones externas.
- El MVCT deberá establecer controles de acceso y autenticación sólidos para restringir el acceso a la información confidencial solo a personas autorizadas. Además, se implementarán soluciones de cifrado y control de contenidos para garantizar la confidencialidad de los datos mientras están en tránsito y en reposo.
- El MVCT deberá realizar evaluaciones regulares de vulnerabilidades y

auditorías de seguridad para identificar posibles brechas en la infraestructura y tomar medidas correctivas de manera proactiva.

### A.8.13 Copia de seguridad de la información

- El MVCT debe asegurar que la información con cierto nivel de clasificación, definida en conjunto por la OTIC 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. Además, se deberá establecer un plan de restauración de copias de seguridad que se probarán a intervalos regulares para asegurar que son confiables en caso de emergencia y retenidas por un periodo determinado.
- La OTIC establecerá procedimientos o un plan de respaldo del MVCT donde se establezcan esquemas de qué, cuándo, con qué periodicidad, la criticidad explícitos de respaldo, número de copias y recuperación de la información que incluyan especificaciones sobre traslado, frecuencia, identificación y definirá con las dependencias los períodos de retención de esta. 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 OTIC deberá realizar y mantener copias de seguridad de la información digital solicitadas por el Líder funcional o Líder técnico.
- La OTIC deberá definir la custodia y almacenamiento de las copias.
- La OTIC deberá tener un inventario y bitácora de las copias que se realizan y de las copias que se restauran.
- La OTIC 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 OTIC deberá generar mecanismos que mantengan la integridad y confidencialidad de las 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 OTIC 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. Si tiene una copia, debe llevarse fuera de la sede o sitio del procesamiento de datos. El traslado de los medios y/o dispositivos debe ser realizado por personal autorizado, considerando las medidas de seguridad.
- Los medios magnéticos con al menos una de las copias con la información crítica deben almacenarse en otra ubicación a las instalaciones dispuestas. 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.8.14 Redundancia de las instalaciones de procesamiento de información

- La OTIC y el operador tecnológico deberán contar con sistemas redundantes para los servicios críticos del Ministerio para garantizar su disponibilidad.
- La OTIC en conjunto con el operador tecnológico deberá poner a prueba los componentes o arquitecturas redundantes implementadas para asegurar que después de una falla el componente funcione.

### A.8.15 Inicio sesión

- La OTIC deberá realizar monitoreo periódico sobre los aplicativos y velar por la generación de los registros de auditoría (logs).
- La OTIC deberá generar registros de auditoría que contengan excepciones o eventos relacionados a la seguridad en los sistemas de información que se consideren.
- La OTIC deberá salvaguardar los registros de auditoría que se generen de cada sistema.
- La OTIC deberá monitorear excepciones o los eventos de la seguridad de información.
- La OTIC deberá monitorear la infraestructura tecnológica para garantizar que estos sean usados para la misionalidad de la entidad.
- La OTIC implementar métodos de inicio de sesión de doble factor.

### A.8.16 Actividades de seguimiento

- Las redes, los sistemas y las aplicaciones que hacen parte de MVCT deberán ser monitoreados por comportamiento anómalo y se tomarán las acciones apropiadas para evaluar posibles incidentes de seguridad de la información.]
- Se deberá realizar monitoreo continuo y análisis regular de los eventos de seguridad, incluyendo registros de acceso, incidentes de seguridad y actividades sospechosas. Además, llevaremos a cabo revisiones periódicas de los controles de seguridad implementados, como firewalls, sistemas de detección de intrusiones y políticas de acceso, para asegurar que estén actualizados y funcionando de manera óptima. Lo anterior se podrá complementar con auditorías para evaluar el cumplimiento de las políticas y estándares de seguridad, e identificar oportunidades de mejora.
- La OTIC será responsable de mantener actualizadas y activas las herramientas de seguridad perimetral que permitan disminuir el riesgo de materialización de incidentes sobre la confidencialidad, disponibilidad e integridad de la información.

### A.8.17 Sincronización de reloj

- La OTIC o el proveedor de tecnología deberá sincronizar los relojes de los servidores con una única fuente de referencia de tiempo (https://horalegal.inm.gov.co/), con el fin de garantizar la exactitud de los registros de auditoría.

### A.8.18 Uso de programas de utilidad privilegiados

- La OTIC 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 programas en sus equipos de cómputo utilitarios que permitan escalar privilegios o evadir controles de seguridadinformáticos.
- La OTIC 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 OTIC deberá generar y mantener actualizado un listado de programas utilitarios privilegiados de la plataforma tecnológica, los servicios de red y sistemas de información.
- La OTIC deberá retirar o deshabilitar los programas utilitarios privilegiados no autorizados de la plataforma tecnológica, los servicios de red y sistemas de información.
- Los programas que puedan invalidar los controles del sistema y la aplicación deberán ser restringidos y controlados.

- Cada programa de utilidad definido por MVCT para uso de sus funcionarios, contratistas y proveedores; debe definir claramente la documentación donde se especifique los niveles de autorización, los roles y privilegios designados a los usuarios de estos.
- Cada programa de utilidad deberá dejar un registro de uso de este a nivel de base de datos que sea gestionada y las acciones adelantadas en la red del MVCT.

### A.8.19 Instalación de software en sistemas operativos

- La Oficina deberá controlar y tener registros de la actualización del software en producción, aplicaciones y librerías de programas propios del MVCT.
- La OTIC deberá usar controles para proteger todo el software implementado y la documentación del sistema.
- La OTIC 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.
- No se deberán alojar en los servidores de producción el código fuente o de desarrollo ni los compiladores.
- La OTIC deberá establecer estrategias de retroceso (rollback) antes de implementar los cambios.
- Todas las instalaciones de software que se realicen sobre equipos del Ministerio deben aprobarla la OTIC, según los procedimientos elaborados para ello.
- 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 OTIC debe desinstalar cualquier software ilegal y registrar este hecho como un incidente de seguridad.
- Corresponde a la OTIC 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 línea base de software definida por la oficina TIC debe revisarse, confirmarse o actualizarse al menos una vez cada cuatro meses.
- La OTIC deberá controlar la instalación y uso de máquinas virtuales y solo podrá realizarse cuando sea necesario para el uso de funciones o labores contratadas y no viole derechos de autor.
- La OTIC podrá inspeccionar el software instalado en los equipos de cómputo y eliminar el software que no cumpla con las condiciones definidas en el

presente manual o documentos de lineamientos inherentes al mismo, previa validación de si existe o no autorización del uso del software en el equipo.

- Solo se permite el uso de software licenciado por el MVCT y/o quien sin requerir licencia comercial sea autorizado por la OTIC. Las aplicaciones desarrolladas al interior del MVCT, en desarrollo de su misión, deberán ser reportadas a la OTIC, para su administración.
- La OTIC es la única dependencia autorizada para la administración del software, que no deberá copiarse, suministrarse a terceros o usarse para fines personales.

**A.8.20 Seguridad en 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 realizarse mediante dispositivos perimetrales e internos de enrutamiento y de seguridad, si se requiere. La OTIC establece el perímetro de seguridad necesario para proteger dichos segmentos, según la criticidad del flujo de la información transmitida.
- La OTIC deberá realizar segmentación de redes para colaboradores y visitantes del MVCT.
- La OTIC 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 OTIC es la responsable de mantener disponible toda la infraestructura de red que soportan los servicios tecnológicos del Ministerio.
- La OTIC debe establecer los procedimientos, guías y demás documentación que permita la gestión de los dispositivos de red del Ministerio.
- LA OTIC es responsable de mantener un registro y monitoreo adecuados para permitir la detección y control de acciones que pueden afectar o son relevantes para la seguridad de la información

**A.8.21 Seguridad de los servicios de red.**

- La OTIC deberá disponer de una zona desmilitarizada o DMZ, entre la red interna del MVCT y la red externa (internet) con el objetivo delimitar conexiones desde la red interna hacia internet y limitar las conexiones desde internet hacia la red interna del MVCT con los siguientes criterios:
    - EL tráfico de la red externa a la DMZ está limitado.
    - El tráfico de la red externa a la red interna 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 monitorearse para 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 deben activar los mecanismos de registro (Logging) y seguimiento para traza de auditorías.
  - Se deben restringir la conexión de los sistemas, servicios y dispositivos a través de mecanismos de control de acceso.
- Se debe promover la confidencialidad, integridad y disponibilidad a través de las redes y sus segmentos tanto en las redes públicas como en las inalámbricas.
- 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 deberá ser administrada desde la OTIC mediante un SSID (Service Set Identifier) único para cada servicio en todas 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 a la Red Corporativa y solo permitirá acceso a Internet; 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 personales a la red Wifi corporativa, para ello se dispondrá de Redes Independientes con acceso a Internet, que deberán aprobarse mediante una solicitud en la mesa de servicios.
- Los colaboradores que requieran acceder a algunos recursos informáticos del MVCT fuera de las 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.
- Los administradores de recursos tecnológicos deben garantizar que los

puertos físicos y lógicos de diagnóstico y configuración de plataformas que soporten sistemas de información estén siempre restringidos y monitoreados para prevenir accesos no autorizados.

**A.8.22 Segregación de redes**

- La OTIC debe definir e implementar mecanismos de separación de las redes del MVCT con base en los niveles de confianza (por ejemplo, acceso público, computadores de escritorio, servidores, etc.), por dependencias (por ejemplo, Grupo de Talento Humano, Grupo de Comunicaciones Estratégicas, oficina de Planeación, Oficina de Tecnologías de la Información y las Comunicaciones) o alguna combinación (por ejemplo, un dominio de servidor que se conecta a múltiples dependencias), asimismo:
    - La OTIC debe mantener separadas la red de datos y la red de voz, con el fin de minimizar el impacto de interceptación de alguna de las dos redes.
    - La OTIC debe establecer una segregación de las redes, separando los entornos de red de usuarios de los entornos de red de servidores y servicios publicados.
    - El acceso remoto a las redes del MVCT se controla mediante conexiones VPN, las cuales deben estar monitoreadas para que se evidencie la desactivación de ésta en el tiempo que se ha definido.
    - Las redes inalámbricas deben estar separadas de las redes LAN, con el fin de garantizar que no se tenga acceso a los recursos o información clasificada y reservada de la Entidad.

**A.8.23 Filtrado web**

- A través del uso de herramientas y soluciones de filtrado web, se controlará y supervisará el acceso a contenido web, bloqueando o restringiendo el acceso a sitios web maliciosos, no seguros o inapropiados. Se establecerán políticas claras y se concientizará a los colaboradores sobre las pautas y restricciones relacionadas con el uso de Internet en el entorno laboral. Además:
    - La OTIC debe regular el acceso a sitios web en función de sus categorías de contenido.
    - Las redes inalámbricas deben tener opciones de filtrado de contenidos Web.
    - Se debe restringir los sitios web que los usuarios del MVCT puede visitar en sus equipos.

## A.8.24 Uso de criptografía

General

- Los responsables de la administración de la plataforma tecnológica deberán utilizar controles criptográficos, para la protección de claves de acceso a sistemas, datos y servicios.
- La OTIC deberá disponer de mecanismos de cifrado en la transmisión de información clasificada o reservada.
- La OTIC 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.
- La OTIC debe establecer y documentar el proceso y controles criptográficos a implementar en los servicios que lo requieran.
- Se deben implementar controles aplicables a la exportación e importación de tecnología criptográfica.
- Con base en el análisis de riesgos, los discos duros externos, memorias USB u otros dispositivos de almacenamiento removible asignados por el MVCT y que contengan información sensible, deben estar cifrados.
- La OTIC apoyará la transmisión de información a otra Entidad o tercero usando controles criptográficos a fin de garantizar la seguridad de la información cuando sea pertinente.
- La OTIC deberá aplicar controles criptográficos para la protección de claves de acceso a sistemas de información.
- Los servidores públicos, contratistas o terceros a los que el MVCT les haya asignado una firma digital o token deben hacer buen uso de estos.
- En caso de presentarse un incidente de seguridad de la información, como perdida, robo u otra afectación relacionada con el uso de las firmas digitales o tokens, se debe reportar inmediatamente por medio de la herramienta mesa de ayuda, al jefe inmediato respectivo y a la OTIC.
- El certificado asignado es personal e intransferible, por lo cual, es responsabilidad del servidor público, contratista o tercero los documentos que firme. Así mismo, el servidor público, contratistas o tercero es responsable de salvaguardar los certificados, claves y tokens asignados.

**Gestión de claves**

- La OTIC definirá y documentará los lineamientos para la generación de claves criptográficas que incluya:
  - Generar claves robustas para sistemas criptográficos y aplicaciones.
  - Generar y obtener certificados de clave pública de manera segura.

- Distribuir claves de forma segura a los usuarios que corresponda, incluyendo Información sobre cómo deben activarse cuando se reciban.
- Almacenar claves, incluyendo la forma de acceso a las mismas por parte de los usuarios autorizados.
- Cambiar o actualizar claves, incluyendo reglas sobre cuándo y cómo deben cambiarse.
- Revocar claves, incluyendo cómo deben retirarse o desactivarse las mismas, por ejemplo, cuando las claves están comprometidas o cuando un usuario se desvincula del MVCT.
- Reponer claves pérdidas o alteradas como parte de la administración de la Continuidad de Operaciones del MVCT, por ejemplo, para la recuperación de la información cifrada.
- Designar un responsable encargado de archivar, respaldar y destruir claves.
- Registrar y auditar las actividades relativas a la gestión de claves.

**A.8.25 Ciclo de vida de desarrollo seguro**

- Las áreas del MVCT propietarias de sistemas de información en conjunto con la OTIC incluirán requisitos de desarrollo seguro en la definición de requerimientos y, posteriormente se asegurarán de que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construidos.
- La OTIC debe establecer metodologías para desarrollar software seguro, que incluyan la definición de requerimientos de seguridad y buenas prácticas, para dar a los desarrolladores una visión clara de lo esperado.
- Las áreas responsables de la administración de los sistemas de información en acompañamiento con la OTIC deben establecer las especificaciones de adquisición o desarrollo de sistemas de información considerando siempre los requerimientos de Seguridad de la Información.
- El área responsable de la administración de los sistemas de información puede definir qué perfiles deben contener los sistemas de información a desarrollar, igualmente, deben aprobar la asignación de estos perfiles cuando sea necesario.
- La OTIC debe liderar la definición de requerimientos de seguridad de los sistemas de información, teniendo en cuenta aspectos como la estandarización de herramientas de desarrollo, controles de autenticación, la arquitectura de aplicaciones, entre otros. Igualmente, el área responsable debe definir los controles de acceso.
- La OTIC debe asegurar que cuando se pretenda implementar un sistema de

información, ya sea propio o de terceros, se someta a un análisis de vulnerabilidades supervisadas que deberán remediarse antes del despliegue en producción por las áreas encargadas.

- La OTIC debe exigir la documentación relacionada con el código fuente para los desarrollos propios y para los casos en que la Entidad adquiera el sistema de información a un proveedor externo
- La OTIC debe exigir toda la documentación de los repositorios y bases de datos de los sistemas de información a los proveedores externos.
- Cuando se contrata desarrollo externo se debe acordar el cumplimiento de los niveles de soporte requeridos por el MVCT. Adicionalmente, se debe acordar la entrega de manuales técnicos, que describan la estructura interna del sistema, así como el diccionario de datos, librerías ejecutables, entidad relación de la base de datos, manuales funcionales, manual del usuario y manual de instalación.
- La OTIC 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 auditoría de los cambios.
    - Se debe asegurar que los sistemas de información adquiridos o desarrollados por terceros cuenten con un acuerdo de licenciamiento en el cual se especifiquen las condiciones de uso del software y los derechos de propiedad intelectual.
    - se debe exigir el suministro de evidencia de que se realizaron pruebas de seguridad al software desarrollado por terceros.
    - Los principios de desarrollo seguro se deben aplicar, en donde sea pertinente, a desarrollos contratados externamente.
    - Se debe asegurar que se hagan pruebas de aceptación del software para verificar el cumplimiento de los requisitos de seguridad acordados.
    - se debe tener en cuenta e incluir en los acuerdos contractuales la necesidad de que el software cumpla con las leyes aplicables.
- La OTIC 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.
  - El MVCT debe contar con ambientes de desarrollo, pruebas y producción separados por máquinas físicas o máquinas virtuales.
- Se debe exigir tanto para desarrollos internos como externos la ejecución de pruebas funcionales que incluyan la evaluación de los requisitos de seguridad de la información y la protección contra vulnerabilidades conocidas.

### A.8.26 Requisitos de seguridad de la aplicación

La OTIC deberá cumplir con los siguientes lineamientos de seguridad:

- 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 OTIC 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.
  - 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 OTIC será la única dependencia autorizada para realizar copia de seguridad del software original.
- El software proporcionado por la OTIC 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 un certificado digital valido.
- 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, se deben generar 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 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 usa la reasignación de

contraseñas, solo se envíe un enlace o contraseñas temporales a cuentas de correo electrónico registradas en los aplicativos, que tendrán un periodo de validez establecido; se deberán forzar el cambio de las contraseñas temporales tras su uso.

- Toda aplicación debe controlar el tiempo inactivo en las sesiones, que deberán cerrarse tras un período de inactividad definido máximo 5 minutos y usar restricciones en los tiempos de conexión para proporcionar una seguridad adicional a las aplicaciones misionales de alto riesgo.

**A.8.27 Principios de arquitectura e ingeniería de sistemas seguros**

- 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 OTIC, con las modificaciones y adquisiciones que se generen.

**A.8.28 Codificación segura**

- El MVCT deberá implementar controles y procedimientos para garantizar que la codificación segura se aplique en todas las fases del ciclo de vida del desarrollo de software. Esto incluye:
  - la adopción de estándares de codificación segura reconocidos,
  - el uso de bibliotecas y frameworks de seguridad confiables,
  - la implementación de pruebas de seguridad, para identificar y corregir posibles vulnerabilidades
- El MVCT deberá promover la concienciación en codificación segura a los desarrolladores de software, para fomentar buenas prácticas y el cumplimiento de las directrices de seguridad.

**A.8.29 Pruebas de seguridad en desarrollo y aceptación.**

- La OTIC 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 OTIC deberá definir controles para que los cambios en los sistemas de información enel 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.8.30 Desarrollo subcontratado**

- La OTIC deberá definir controles para que los sistemas adquiridos externamente cumplancon 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.
  - acuerdos de depósito en garantía para el código fuente del software, por medio de entregas parciales y finales, código que debe estar explicado en sus líneas de desarrollo de acuerdo con la lógica de desarrollo utilizada de manera que no haya una vinculación obligatoria entre desarrollador y posibles futuras modificaciones.
- La OTIC deberá contemplar en los cambios y en los nuevos sistemas de información, pruebas asociadas a seguridad de la información.

**A.8.31 Separación de los entornos de desarrollo, prueba y producción**

- La OTIC deberá realizar la separación de ambientes de desarrollo, pruebas y producción, los cuales deberán estar separados de manera física y lógica.
- La OTIC deberá definir y documentar los lineamientos a seguir para la transferencia entre ambientes.
- La OTIC deberá utilizar datos que no sean sensibles para el MVCT, en los ambientes de prueba y desarrollo.
- La OTIC 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 OTIC deberá garantizar que los desarrolladores realicen su trabajo exclusivamente en el ambiente de desarrollo y nunca en los ambientes de pruebas o producción.

**A.8.32 Gestión del cambio**

- La OTIC debe establecer un procedimiento que permita asegurar la gestión de cambios normales y de emergencia en infraestructura, aplicativos y servicios tecnológicos para desarrollarlos bajo estándares de eficiencia, seguridad, calidad y determinar los responsables y tareas en la gestión de cambios.
- La OTIC debe establecer un comité de cambios, quien se encargará de evaluar, aprobar o negar la implementación de los cambios.
- Cuando la OTIC desarrolle o realice mejora a las aplicaciones o sistemas e información, deberán definir controles para que los cambios realizados se documenten, considerando la integridad de los sistemas y/o aplicaciones desde las primeras etapas de diseño y mediante mantenimientos posteriores.
- La OTIC 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 OTIC 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 propietario 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 OTIC deberá conservar el software original cuando se hayan realizado cambios en los paquetes de este.
- La OTIC deberá definir controles para la transferencia de información a través de redes públicas para las aplicaciones del MVCT.
- La OTIC 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.

**A.8.33 Información 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 de los 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 datosde prueba no deben contener información que permitan la identificación de la persona natural o jurídica a la que pertenezca la información.
- La OTIC deberá evitar durante la ejecución de pruebas en ambientes de desarrollo el usode datos que contengan información personal o información sensible del MVCT que este contenida en el ambiente de producción de las aplicaciones.
- La OTIC deberá tener en cuenta controles de acceso a los ambientes de producción y deprueba.

**A.8.34 Protección de los sistemas de información durante las pruebas de auditoría**

- La OTIC, como segunda línea y líder de la política de seguridad digital, planificará actividades con auditorias de los sistemas críticos en producción, limitando el acceso al sistema de información y a los datos de solo lectura (si se deberá acordar previamente), determinando tareas, responsables y

se deberán realizar fuera del horario laboral.

- La OTIC, 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 con 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.

ANEXO No.2

# Anexo No.2

# GUIA DE USO Y ACCESO A RECURSOS DE TIC

El presente anexo se establece para apropiar a la comunidad de usuarios del MVCT en la importancia y sensibilidad en el uso de los sistemas información, uso y administración de los activos de información y servicios críticos con el fin de:

- Propender que los servicios tecnológicos y de comunicaciones se ofrezcan con calidad, confiabilidad, integridad, disponibilidad y eficiencia.
- Concientizar a la comunidad de usuarios del MVCT sobre la importancia del uso racional y seguro de la infraestructura informática.
- Cuidar y proteger los recursos tecnológicos y evitar el comportamiento inescrupuloso y uso indiscriminado de los mismos.
- Gestionar el almacenamiento de información y el uso de espacio en los repositorios y servicios de Almacenamiento dispuestos en el MVCT.
- Disminuir los riesgos en seguridad de la información.

ANEXO No.2

# 1. GUIA GENERAL PARA LOS USUARIOS DE LOS SERVICIOS TECNOLÓGICOS DEL MVCT

## 1.1. Uso de los Recursos Tecnológicos

La infraestructura tecnológica asignada a funcionarios y contratistas se considera de propiedad del Ministerio de Vivienda, Ciudad y Territorio de Colombia (MTCV) y se empleará de manera exclusiva y bajo la completa responsabilidad por los mismos, únicamente para el desempeño de las funciones del cargo o las obligaciones contractuales pactadas. Por tanto, no pueden ser utilizados con fines personales o por terceros no autorizados por la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC).

Solo se permite el uso de software licenciado por el Ministerio y/o quien, sin requerir licencia, sea autorizado por la OTIC.

Las únicas personas autorizadas para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos, como destapar, agregar, desconectar, retirar, revisar y/o reparar sus componentes, son el personal técnico asignado a la Mesa de Ayuda

La OTIC realizará monitoreo sobre los dispositivos de almacenamiento externos conectados a los equipos del MVCT, como son: USB, CD-ROM, DVD, Discos Duros externos, entre otros, con el fin de prevenir o detectar fuga de información.

La única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro será la Subdirección de Servicios Administrativos. En tal virtud, toda reasignación de equipos deberá ajustarse a los procedimientos y competencias de la gestión de Recursos Físicos de la Entidad.

La pérdida o daño de elementos o recursos tecnológicos, o de alguno de sus componentes, deberá informarse de inmediato a la OTIC por el funcionario o contratista asignado.

La pérdida de información deberá informarse a la OTIC, a través de la Mesa de Servicios como incidente de seguridad.

Todo incidente de seguridad que comprometa la disponibilidad, integridad o confidencialidad de la información física o digital deberá ser reportado a la mayor brevedad posible a la Mesa de Servicios, a través de los Medios de Comunicación dispuestos.

Todo acceso a la red del Ministerio mediante elementos o recursos tecnológicos no institucionales deberá ser informado la OTIC.

ANEXO No.2

Las conexiones a la red wifi para funcionarios y contratistas del MVCT son administrados desde la OTIC y la autenticación deberá ser con usuario y contraseña asignados.

- **Recomendaciones.**
  - En caso de que el funcionario o contratista deba hacer uso de equipos personales, estos deberán cumplir con la legalidad del Software instalado, antivirus licenciado y actualizado y solo podrá conectarse a la red del MVCT identificada como Colaborador, una vez esté avalado por la OTIC.
  - Los usuarios no deben guardarse en los discos duros de computadores de escritorio, portátiles o discos virtuales de red, archivos de vídeo, música y fotos que no sean institucionales o que atenten con los derechos de autor o propiedad intelectual de estos.
  - La OTIC es la única dependencia autorizada para administrar el software, que no deberá copiarse, suministrarse a terceros ni usarse para fines personales.
  - Los equipos deben quedar apagados cada vez que el funcionario o contratista no se encuentre en la oficina o durante la noche, esto, con el fin de proteger la seguridad y distribuir bien los recursos de la Entidad, siempre y cuando no vaya a realizar actividades vía remota.
  - Los usuarios deberán almacenar toda la información de usuario en el espacio o disco de One Drive, para tal efecto deben consultar con el personal técnico de la OTIC cualquier duda o situación que se presente con el equipo de cómputo.
  - No se pueden exponer a terceros equipos de cómputo, en ausencia del responsable, la sesión de bloquearse para evitar fuga de información.

- **Prohibiciones.**
  - No está permitido fumar, ingerir alimentos o bebidas en el área de trabajo donde se encuentren elementos tecnológicos o información física que pueda estar expuesta a su daño parcial o total y por ende pérdida de la integridad de esta.
  - No está permitido realizar conexiones o derivaciones eléctricas que pongan en riesgo los elementos tecnológicos por fallas en el suministro eléctrico a los equipos de cómputo, salvo en aquellos casos que sean autorizados por el grupo de Recursos Físicos.
  - No está permitido realizar conexiones o derivaciones a la Redes de Datos de las diferentes sedes de la Entidad.

- Acceder a información perteneciente a otro Usuario sin autorización.
- Realizar copias o modificaciones de información no autorizadas.

### 1.2. Uso De Equipos Portátiles Asignados a funcionarios y contratistas del MVCT.

Las computadoras portátiles asignadas, que se requieran usar por fuera de la entidad, deben serlo tomando las medidas de seguridad necesarias y no pueden ser utilizados en actividades distintas a las laborales.

En caso de tener asignado un computador portátil, se deben tomar las medidas preventivas de seguridad necesarias, así mismo, mantener el computador con guaya de seguridad o guardar el equipo bajo llave, con el fin de prevenir la pérdida de la información y del bien.

No se pueden dejar expuestas a la utilización de terceros equipos de cómputo, si no el responsable, la sesión debe bloquearse para evitar fuga de información.

Si la conexión a red utilizada es diferente a la red de la entidad, se debe realizar la conexión a una red segura (para red inalámbrica debe utilizar seguridad WPA o WPA2).

En caso de viaje, las computadoras portátiles se deben llevar como equipaje de mano, usando un maletín adecuado.

Manejar la información y los datos de acuerdo con el apartado "*Uso de repositorios de Información*" incluido en este documento.

Si se maneja información reservada, informar a la OTIC para solicitar la implementación de cifrado del disco duro, si no se ha implementado.

En los equipos portátiles de propiedad del MVCT, los funcionarios y contratistas no pueden realizar ningún cambio o alteración física de algún componente.

- **Prohibiciones**
  - Está prohibido almacenar información personal en los equipos de cómputo asignados por el ministerio de Vivienda Ciudad y Territorio.
  - Está prohibido realizar instalación de aplicaciones no autorizadas por la Oficina de las TIC.
  - Está prohibido reinstalar el sistema operativo del dispositivo por parte del usuario.

ANEXO No.2

### 1.3. Uso de dispositivos personales que accedan a información o redes del MVCT.

Los funcionarios o contratistas que hagan uso de dispositivos personales tales como computadores, tabletas, celulares, Smartphones, etc., para acceder a información del MVCT deberán:

- Solicitar la autorización a la Oficina de las TIC a través de la Mesa de Ayuda y diligenciar el formato GT-F-14 (compromiso de confidencialidad), aceptando el cumplimiento de la política de dispositivos personales.

Aceptar las recomendaciones de seguridad del dispositivo establecidas por la OTIC mientras se acceda a información del MVCT.

- Los colaboradores que acepten el acceso a las redes de la entidad con sus equipos personales en modalidad de BYOD deben demostrar que los dispositivos contienen software legal y que no va en contravía de la propiedad intelectual y que la utilización de software ilegal trae consigo violación en protección de propiedad intelectual y por consiguiente consecuencias como responsabilidades civiles y penales según sea el caso.
- El licenciamiento del software, sistemas operativos y aplicaciones en los dispositivos personales de los colaboradores es responsabilidad exclusiva de estos. En caso de una revisión por Mesa de Ayuda revele licencias no legales, se informará al proveedor el usuario y la máquina involucrados. Sin embargo, esto no exime la obligación de utilizar software legalmente adquirido, conforme a la Ley 603 de 2000 o sus normas sucesoras.
- Usar software de antivirus actualizando cuando aplique.
- Establecer un mecanismo de control de acceso como contraseña superior a 8 caracteres, un patrón de seguridad de al menos 7 puntos de contacto, o huella digital.
- Configurar el bloqueo de pantalla para un mínimo de 2 minutos de inactividad.
- Los colaboradores que acepten el acceso a las redes de la entidad con sus equipos personales, una vez terminada su relación contractual con la entidad, garantizarán el borrado seguro de la información a su cargo.

▪ **Prohibiciones**

- Está prohibido almacenar información de la Entidad en los equipos de cómputo personales.

ANEXO No.2

### 1.4. Mecanismos de Seguridad de la Información.

Con el fin de evitar riesgos de seguridad de la información como la fuga y/o pérdida de información, todos los equipos portátiles y estaciones de escritorio cuentan con mecanismos de actualización constante de software de protección de dispositivos finales de usuario (Antivirus). Cualquier empleado que tenga bajo su responsabilidad algún computador portátil asignado por el MVCT y que dicho activo no esté conectado de forma permanentemente a la red de la entidad o a Internet, será responsable de solicitar a la OTIC las actualizaciones de las herramientas de protección para su dispositivo asignado.

- **Recomendaciones**
  - El escaneo automático de archivos nuevos y/o unidades de almacenamiento externas (discos, memorias, etc.) permanece activo. Si el software antivirus detecta un riesgo de infección, el usuario debe atender las recomendaciones realizadas por él y comunicarse con la Mesa de Ayuda si se requiere acceso al archivo/carpeta infectada.
  - Para prevenir infecciones por virus informático los empleados del MVCT, no deben hacer uso de ningún software, que no haya sido proporcionado y/o validado por la Mesa de Ayuda.
  - Todos los archivos de computadora que sean proporcionados por personal externo o interno en relación con programas de software, bases de datos, documentos, hojas de cálculo entre otros que tengan que ser descomprimidos, en las maquinas del MVCT, serán analizados por las herramientas de seguridad y estas los bloquearan o destruirán si encuentran algún riesgo de seguridad para la Entidad.
  - Cualquier empleado que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y realizar una solicitud por la herramienta de gestión de mesa de servicio, con el fin de que este sea revisado por la OTIC, para la detección y erradicación del virus.
  - Todos los medios removibles y otros medios de almacenamiento electrónico sobre un computador infectado no deberán ser utilizados sobre otro computador hasta que el virus haya sido removido de manera exitosa.
  - Si hay un computador infectado con algún virus, se retirará de la operación para su revisión por parte de la Mesa de Ayuda.

- Debido a la complejidad de algunos virus ningún funcionario o contratista del MVCT, debe intentar eliminarlos de las computadoras. La Mesa de Ayuda será la encargada o responsable de llevar a cabo las acciones para la remoción del virus y garantizar la pérdida de información, minimizar los daños y el tiempo fuera de servicio del computador infectado.

- **Prohibiciones**
  - Los usuarios de los equipos de cómputo de la entidad no deberán detener o cancelar los procesos automáticos de actualización de las Herramientas de Seguridad de Usuario Final.
  - Ningún empleado del MVCT, debe intencionalmente escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir programas, software o códigos de computadora diseñados para auto replicarse, dañar, o extraer información. El incumplimiento de este lineamiento será considerado una falta grave.
  - Ningún empleado o personal externo podrá descargar software o sistemas, que generen correos masivos, funcionen como pasarelas, proxys, túneles, software de mensajería instantánea o que permitan el acceso a redes de comunicaciones externas, sin la debida autorización de la OTIC.
  - Los empleados no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por el MVCT en su plataforma tecnológica (Antivirus, Outlook, Office, Navegadores u otros programas).

### 1.5. Acceso a la Red y a los Recursos Informáticos

#### 1.5.1. Para funcionarios y contratistas

Cualquier equipo que se conecte a la red del Ministerio por red cableada o inalámbrica debe cumplir con condiciones mínimas de protección como son: Sistema Operativo soportado y licenciado con las últimas actualizaciones de seguridad aplicadas, software Antivirus actualizado.

Cada usuario es el único responsable de la administración y el buen uso de su nombre de usuario y contraseña de red, por lo tanto, será responsable de las acciones realizadas por terceros quienes conozcan su clave de ingreso a las redes corporativas. Igualmente será responsable de las sesiones que deje abiertas con su usuario activo.

ANEXO No.2

Para efectos de realizar control y seguimiento de la seguridad informática, el equipo de soporte de la OTIC de la entidad podrá monitorear equipos, sistemas y tráfico de red en cualquier momento.

La OTIC establecerá los mecanismos necesarios para proveer la disponibilidad de las redes y los servicios que dependen de ellas; así, dispondrá y vigilará los de seguridad para proteger la integridad y la confidencialidad de la información del MVCT.

Los equipos personales conectados por la red de colaboradores deberán contar con el sistema operativo licenciado y actualizado, con un software antivirus actualizado y no deberá contar con ningún software que permita evadir los controles de seguridad tecnológica del MVCT.

### 1.5.2. Para proveedores o terceros

Para los casos en que los equipos sean de propiedad de los proveedores y se utilicen como parte de una solución y que se conecten a la Red LAN del MVCT, el proveedor deberá diligenciar el formato GT-F-14, carta de compromiso de confidencialidad y entregarla a la OTIC.

El proveedor o tercero deberá entregar las direcciones MAC de los equipos de la solución antes de ser conectados a la red LAN del MVCT.

El proveedor deberá notificar a la OTIC los puertos TCP/UDP a utilizar, para el funcionamiento de su aplicación.

Los equipos del proveedor deben tener instalado únicamente el software requerido para que la solución funcione con su respectivo licenciamiento, el cual debe ser reportado a la OTIC.

Los equipos del proveedor no deben contar con acceso a Internet diferente al asignado por el MVCT, ni con ninguna conexión remota, lo cual será verificado por la OTIC.

El proveedor deberá asignar un usuario administrador con los conocimientos avanzados en la solución, quien se encargará de atender las fallas y dar el soporte técnico de la solución en sitio.

- **Recomendaciones**
  - Cada equipo de cómputo está habilitado para conectar a un único punto de red, si se requiere conectar un equipo o cualquier dispositivo de red a otro punto, se debe solicitar a la OTIC.
- **Prohibiciones**
  - La conexión a cualquier punto de red está restringida.

- Para efectos de realizar control y seguimiento de la seguridad informática, el equipo de soporte de la OTIC de la entidad podrá monitorear equipos, sistemas y tráfico de red en cualquier momento.

### 1.6. Acceso y Uso de Internet

La Internet es el método más común de contagio y de riesgo informático que una compañía puede enfrentar. Razón por la que deben seguirse las siguientes acciones para proteger las redes y los sistemas de información:

- La OTIC establecerá políticas de navegación basadas en categorías y niveles de usuario por jerarquía y funciones, que se implementarán en el MVCT.
- El acceso a Internet solo debe usarse para fines laborales e institucionales y puede servir de gestión, desarrollo, consulta y comunicación de actividades relacionadas con los procesos del MVCT.
- Los servicios a los que un determinado usuario pueda acceder en internet dependerán del rol o funciones que desempeña en el MVCT y para las cuales esté formal y expresamente autorizado.
- Todo usuario es responsable de informar a la OTIC, los contenidos o accesos a servicios que no le estén autorizados y/o no correspondan a sus funciones dentro del MVCT.
- Los dispositivos personales propiedad del usuario tales como: Computador Portátil, Celulares Smartphone, Tablets, Ipads y similares, solo podrán conectarse a las redes inalámbricas asignadas para los mismos.

El MVCT se reserva el derecho a monitorear los accesos, y el uso del servicio de Internet de todos sus funcionarios o contratistas y verificar cualquier documento enviado o recibido a través de conexiones en línea y que sea guardado en los computadores del MVCT.

- **Prohibiciones**

Está prohibido a los usuarios, realizar las siguientes acciones:

- Hacer uso de las redes o equipos de cómputo del MVCT para redactar, transmitir o recibir vía Internet, información o contenido que pudiera ser discriminatorio, ofensivo, obsceno, amenazante, intimidante o destructivo para cualquier individuo u organización. Ejemplos de contenido inaceptable incluyen, entre otros, comentarios en general, imágenes de contenido sexual o discriminación racial.

- El acceso a páginas de dudoso contenido o autoría, sitios pornográficos, sitios religiosos dedicados a difundir las creencias de alguna religión o secta en particular, acceso a sitios web de alzados en armas o de grupos terroristas a nivel nacional o internacional dedicados a difundir temas relacionados con violencia.
- Utilizar el canal de conexión a Internet para descargar música, videos y archivos ejecutables.
- Está prohibido acceder a páginas web, portales, sitios web y aplicaciones web que no hayan autorizado el MVCT.
- Está expresamente prohibido el envío y descarga de cualquier tipo de software o archivos de fuentes externas, y de procedencia desconocida.
- Está expresamente prohibida la propagación de virus o cualquier tipo de código malicioso

### 1.7. Acceso a los Sistemas de Información

Todos los funcionarios y contratistas del MVCT son responsables de la protección de la información que acceden y/o procesan, así como de evitar su pérdida, alteración, destrucción y uso indebido, para lo cual se dictan los siguientes lineamientos:

- El acceso a los sistemas de información que provee el MVCT se da a los usuarios del MVCT como medio de soporte para obtener la información necesaria para realizar óptimamente sus actividades con herramientas tecnológicas.
- Todo tipo de información transmitida o recibida por un sistema computacional o de comunicación se considera parte de los registros oficiales MVCT y cumple las normas y restricciones consignadas en este documento. Por ello, el usuario deberá asegurarse que la información de los mensajes de e-mail, chat y en otras transmisiones es precisa, apropiada, ética y constructiva.
- El usuario debe velar por la confidencialidad de su(s) contraseña(s), usada(s) para el acceso a los sistemas de información de la entidad.
- Las credenciales de acceso a la red y a los recursos informáticos (Usuario y Clave) son de carácter estrictamente personal e intransferible; los funcionarios y contratistas no deben revelarlas a terceros ni utilizar claves ajenas.
- Todo funcionario y contratista es responsable de los registros y modificaciones de información que se hagan a nombre de su cuenta de usuario.

- Cuando un funcionario o contratista cesa en sus funciones o culmina la ejecución de contrato en MVCT, todos los privilegios sobre los recursos informáticos otorgados le serán suspendidos inmediatamente; la información del empleado y/o contratista serán almacenados en un repositorio de los servidores de la Entidad.
- Las aplicaciones generadas o adquiridas por el MVCT en desarrollo de su operación institucional y que no fueron desarrollados por el MVCT deben ser reportadas a la OTIC.

- **Recomendaciones**

  - Todo funcionario y contratista es responsable del cambio de clave de acceso a los sistemas de información o recursos informáticos periódicamente.
  - En ausencia del funcionario o contratista, el acceso a la estación de trabajo se bloqueará con una solicitud a la OTIC a través de la Mesa de Ayuda, para evitar la exposición de la información y el acceso a terceros, que puedan generar daño, alteración o uso indebido, y a la suplantación de identidad, el Grupo de Talento Humano debe reportar cualquier novedad de los funcionarios y el Supervisor del Contrato.
  - Cuando un funcionario o contratista cesa en sus funciones o culmina la ejecución de contrato en MVCT, el supervisor o jefe inmediato es el encargado de la custodia de los recursos de información, incluyendo la cesión de derechos patrimoniales de acuerdo con la normativa vigente.

- **Prohibiciones**

Está prohibido a los usuarios de los sistemas de información del MVCT, realizar las siguientes acciones:

- Ingresar o tratar de ingresar a sistemas de información a los cuales un usuario no tiene acceso.
- Exportar información de los sistemas de información del MVCT y hacer mal uso de la misma (vender, divulgar, reproducir, entre otras), a personal ajeno del Ministerio sin autorización del propietario del activo de información.
- Modificar o eliminar información de los sistemas de información.

ANEXO No.2

### 1.8. Uso de Repositorios de manejo de la Información

El Ministerio cuenta con los siguientes repositorios de información, que deben usarse según la información tratada. A continuación, se identifica el propósito y lineamiento de uso de los repositorios del Ministerio:

| REPOSITORIO | | PROPOSITO |
|---|---|---|
|  | **Domusfile**<br>Servidor de Archivos | • Enfocado a guardar archivos e **información histórica** de consulta permanente.<br>• Información organizada en **Carpetas**.<br>• **Información** por **áreas**, histórica, retención por años.<br>• **Búsqueda lenta** y compleja.<br>• **Acceso controlado** por carpeta. |
|  | **GesDoc**<br>Gestor Documental | • Enfocado a la **organización documental** y búsqueda rápida.<br>• **Información** de la **entidad** organizada por **tipos** de **documento**.<br>• **Búsqueda** y visualización **rápida**<br>• **Acceso controlado** por tipo de documento. |
|  | **SharePoint**<br>Almacenamiento en Nube | • Enfocado a **trabajo colaborativo**, varios usuarios editando y compartiendo información de interés común.<br>• **Información** organizada por **grupos** de **trabajo**, o por temas de trabajo común.<br>• **Acceso controlado** para el equipo de trabajo, según rol asignado. |
|  | **OneDrive**<br>Almacenamiento en Nube | • Enfocado a guardar **información** de uso **Individual en la entidad**, archivos de trabajo, etc.<br>• Disco duro local sincronizado en la nube.<br>• Acceso controlado para el propietario de la unidad en la nube.<br>• **Archivos privados**. |

**¿Que guardar en cada repositorio?**:

**Domusfile**: Archivos del área con vigencia al año en curso.

ANEXO No.2

**Gesdoc**: Información por tipo de documentos.
**Sharepoint**: Archivos a trabajar por grupos de trabajo.
**OneDrive**: Información por empleado (funcionario o contratista) de trabajo diario.

- **Recomendaciones y Prohibiciones**

  - Está expresamente prohibido el almacenamiento en los discos duros de computadoras de escritorio, portátiles o discos virtuales (Onedrive, etc.) archivos de vídeo, música y fotos que no sean de carácter institucional o que atenten contra los derechos de autor o propiedad intelectual de los mismos.
  - La pérdida de información deberá ser informada con detalle a la oficina de tecnologías de la información a través de la mesa de servicios como incidente de seguridad.

En el caso que el funcionario o contratista haga uso de sus equipos personales y estos terminen su relación de trabajo con el Ministerio, la información producto de su trabajo debe ser entregada a su supervisor o jefe inmediato y la información eliminada de los equipos personales.

### 1.9. Uso de Office 365

Las herramientas de Office 365 como: outlook, Teams, OneDrive, SharePoint y las aplicaciones conexas, están declaradas en la presente guía como los medios oficiales de comunicaciones unificadas para el envió de correo electrónico, mensajes de texto, mensajes multimedia, compartir archivos, publicar información y todos los medios electrónicos disponibles en estas herramientas para el trabajo colaborativo de los funcionarios y contratistas del MVCT, todo lo anterior está acompañado de los siguientes deberes y obligaciones:

- Emplear la cuenta de usuario exclusivamente para los fines asignados.
- Utilizar su cuenta en forma individual, sin compartirla y vigilar que nadie pueda emplearla cuando tenga abierta una sesión de trabajo.
- Informar al administrador o coordinador del sistema en forma inmediata si tiene conocimiento de cualquier uso indebido de su cuenta o de su medio de acceso al sistema.
- Informar al administrador del sistema si detecta alguna anomalía en el mismo.
- Todo usuario deberá respetar la naturaleza confidencial del acceso de un usuario o cualquier otra información que pueda caer en su poder, ya sea como parte de su trabajo o por accidente.

- Toda la información que se comparta a través de estos medios es de titularidad exclusiva del MVCT.
- El contenido de los mensajes enviados y recibidos se considera confidencial y solo perderá este carácter en casos de investigaciones administrativas, judiciales o incidentes relacionados con seguridad informática.
- Para los mensajes de correo electrónico a quien un mensaje individual de correo puede ser enviado se limitará a Veinticinco (25) cuentas de correo internas y/o externas.

En caso de requerirse envío de correos masivos, el usuario deberá comunicarse con el grupo de Soporte y Apoyo Informático.

- **Prohibiciones**
  - Hacer proselitismo de ideas políticas, gremiales o religiosas.
  - Publicar contenidos que promuevan intolerancia, violencia, racismo o vicios.
  - Publicación de links o vínculos a páginas externas que vayan en contra de los principios y valores del MVCT.
  - Usar los servicios de Comunicaciones Unificadas con propósitos personales o comerciales.
  - Envió de comunicaciones masivas internas o externas.
  - Reproducción y envío de mensajes en cadenas o similares.

### 1.10. Conexiones VPN

El acceso a la red corporativa del MVCT a través de una conexión VPN para acceso o trabajo remoto, solo puede ser autorizado a través del jefe del área o grupo.

Cada usuario es el único responsable de la administración y el buen uso de su nombre de usuario y contraseña asignada para conexión VPN, por lo tanto, será responsable de las acciones realizadas por terceros quienes conozcan su clave de ingreso a las redes corporativas.

Para efectos de validar la seguridad, realizar monitoreo y certificar la estabilidad del servicio de las conexiones VPN, la OTIC podrá monitorear equipos, sistemas y tráfico de red que circule por la conexión VPN en cualquier momento.

ANEXO No.2

## 2. GUIA DE CREACIÓN CUENTAS DE USUARIO PARA EL USO DE LOS SISTEMAS Y APLICACIONES EN EL MVCT.

Actualmente en el MVCT existen dos tipos de cuentas de correo electrónico corporativo:

**Cuenta de Correo Institucional de uso Individual**: Esta cuenta es asignada a funcionarios y contratistas del MVCT.

**Cuenta de Correo Institucional de uso general:** Esta cuenta es asignada a cargos o dependencias del MVCT.

### 2.1. Solicitud para la creación del Correo.

Cada dependencia debe de solicitar a través de la aplicación de Mesa de Ayuda en la opción de cuentas de usuario, la creación de cada cuenta de correo, según procedimiento GTI-P-06.

#### 2.1.1. Condiciones especiales.

**Cláusula de actividad de cuenta:** la cual establece que pasados 60 días de inactividad de las cuentas de correo de uso individual, se pasarán a bloqueo y posteriormente pasados 30 días, serán eliminadas. Solo las cuentas de correo de uso general se respaldarán según la tabla de retención documental establecida para correo electrónico.

**Acuerdo de Confidencialidad de la Información:** Debido a la naturaleza del trabajo, se hace necesario que éstas manejen información confidencial y/o información sujeta a derechos de propiedad intelectual, antes, durante y en la etapa posterior, por ello al momento de crear una cuenta de correo, el usuario deberá firmar dicho acuerdo en conjunto con el encargado de la dependencia.

**Aceptación de deberes y responsabilidades de la cuenta de Correo:** Al momento de recibir la notificación de la creación de la cuenta de correo Institucional el usuario debe verificar que toda la información este correcta y firmar el formato que llega con el correo de aceptación de deberes y responsabilidades. Se debe de verificar que se encuentren todos sus campos completos y las firmas correspondientes.

### 2.2. Asignación del ID USER.

Se asigna con la primera letra del primer nombre, seguido del apellido, si existe dicho ID, corresponderá a las primeras letras del primer y segundo nombre seguido del apellido; se anexará la primera letra del segundo apellido al final del ID si persiste un

ID igual. Se asignará una contraseña por defecto, con la recomendación de que el usuario debe de cambiarla al ingresar por primera vez a la cuenta. Este ID solo será modificable en caso de presentarse una palabra o frase que pueda herir susceptibilidades.

El usuario debe cambiar la contraseña creada por defecto al ingresar por primera vez y periódicamente según la solicitud e indicaciones del sistema.

El ID USER asignado a los usuarios no debe ser utilizado para la inscripción a servicios externos a la entidad, a menos que sea para la ejecución de sus funciones.

## 3. GUÍA PARA LA PROTECCIÓN DE LA INFORMACIÓN

Cada usuario de la entidad es responsable del manejo de la información desarrollada durante su ejercicio laboral.

La información debe guardarse en la ubicación de Sharepoint o OneDrive de cada usuario.

En el caso que el usuario maneje información muy sensible o critica para la entidad, el usuario o su jefe inmediato debe solicitar una copia adicional de esta información al Grupo de Apoyo Tecnológico del Ministerio.

### 3.1. Respaldo de archivos Locales en máquinas de usuario

Es responsabilidad del usuario clasificar la información para tener un repositorio de información organizado y efectivo vinculado a su cuenta de Onedrive. La clasificación debe tener archivos y documentos de la dependencia y que son de importancia para la misma; la información como música, fotos, videos y demás archivos de tipo personal, no debe estar en los equipos del MVCT ya que podrá ser eliminada.

### 3.2. Respaldo Cuentas de Correo

La información contenida en las cuentas de correo institucional de uso general es de vital importancia para trazabilidad de la correspondencia interna externa del MVCT; por ello es muy importante la generación, almacenamiento y custodia de las copias de respaldo del correo electrónico.

El usuario del correo es responsable de depurar el correo enviado y recibido para mantener funcionando su buzón, y el sistema genera alertas automáticas que le permiten al usuario realizar esta labor de depuración.

ANEXO No.2

Si el usuario requiere una copia por llenado de la capacidad de almacenamiento del buzón asignado, deberá comunicarse con la mesa de servicio mediante un requerimiento de soporte técnico para realizar la respectiva copia de respaldo. Para las cuentas institucionales de uso individual, el usuario será responsable de suministrar el medio requerido para la respectiva copia de respaldo y custodiará la copia generada.

Solo las cuentas de correo general serán respaldadas de acuerdo con la tabla de retención documental establecida para correo electrónico y es el Grupo de Apoyo Tecnológico el único responsable de la custodia de estas copias de respaldo. Cada copia de respaldo deberá ir acompañada del formato de Backup GSI-F11 debidamente diligenciado y firmado.

### 3.3. Uso de correo electrónico

Del uso del correo electrónico. El correo electrónico institucional es una herramienta de apoyo a la ejecución de funciones y obligaciones de los empleados públicos y contratistas del Ministerio de Vivienda, Ciudad y Territorio, cuyo uso se facilitará en los siguientes términos:

- El servicio de correo electrónico designado por la Oficina de Tecnologías de la Información, con el dominio @minvivienda.gov.co, es el único autorizado para gestionar y transmitir información institucional. Este servicio cumple con los requisitos técnicos y de seguridad, protegiendo contra amenazas como virus, spyware y otros programas maliciosos.
- El correo electrónico institucional debe usarse solo para intercambiar mensajes institucionales. No se permite su uso con propósitos personales, comerciales, económicos u otros ajenos a los objetivos de la entidad.
- Se prohíbe el envío de correos masivos (más de 30 destinatarios) excepto en casos específicos autorizados. Los correos masivos deben cumplir con las normas de comunicación e imagen corporativa y solo pueden ser enviados por ciertos despachos y la Oficina de Tecnologías de la Información durante ventanas de mantenimiento.
- Cualquier mensaje de correo electrónico enviado por el Ministerio a través de plataformas externas debe utilizar la cuenta de la entidad y el dominio @minvivienda.gov.co para evitar ser clasificado como spam o suplantación de correo.
- Para respaldar la gestión del correo electrónico de los directivos, se permite la delegación del buzón correspondiente, solicitada por el titular para especificar

los colaboradores autorizados a responder en su nombre y prevenir suplantaciones.

- Cualquier mensaje de spam, cadena o contenido sospechoso debe ser reportado de inmediato a la Oficina de Tecnologías de la Información a través de la Mesa de Servicios como un incidente de seguridad. Se deben seguir las indicaciones recibidas para su tratamiento, ya que podría contener virus u otro contenido perjudicial.
- La cuenta de correo institucional no debe revelarse en sitios publicitarios o en cualquier plataforma no autorizada por la entidad, para preservar su integridad y seguridad.
- Se prohíbe el uso del correo para transmitir contenidos insultantes, ofensivos, injuriosos, obscenos, violatorios de los derechos de autor o que atenten contra la integridad moral de personas o instituciones.
- Cuando la información transmitida esté catalogada como clasificada o reservada, el cifrado de los mensajes de correo electrónico institucional será obligatorio, según lo establecido en la ley y el inventario de activos de información.
- Queda expresamente prohibido distribuir, copiar o reenviar información del Ministerio a través de correos personales o sitios web no autorizados en el marco de las funciones u obligaciones contractuales, así como, la información clasificada y reservada.

## 4. INCUMPLIMIENTO A LAS POLÍTICAS Y PROTOCOLOS DE SEGURIDAD INFORMÁTICA.

El incumplimiento a cualquiera de las políticas establecidas en este documento acarrearía las sanciones disciplinares y legales a que se sucedieran según la legislación vigente.

ANEXO No.2

## 5. DEFINICIONES Y ABREVIATURAS

- **Aceptación del riesgo**: decisión de asumir un riesgo.
- **Activo:** Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas) que tienen un valor para la entidad.
- **Activos asociados:** son aquellos que están directa o indirectamente relacionados con la seguridad de la información. Estos activos pueden incluir:
    1. Activos de información: Cualquier información que una organización posea o controle, como bases de datos, documentos, propiedad intelectual y datos personales.
    2. Activos físicos: Elementos tangibles que son necesarios para el procesamiento, almacenamiento o transmisión de información, como servidores, ordenadores, dispositivos móviles y equipos de red.
    3. Activos humanos: Personal que tiene acceso o es responsable de la gestión de sistemas de información y datos, incluidos empleados, contratistas y proveedores de servicios de terceros.
    4. Activos de software: Aplicaciones, programas y sistemas de software que se utilizan para procesar, almacenar o transmitir información dentro de una organización.
    5. Activos de infraestructura: La infraestructura física y virtual que soporta los sistemas y servicios de información, incluyendo centros de datos, redes y servicios en la nube.
    6. Activos financieros: Los recursos asignados para apoyar las iniciativas de seguridad de la información, incluidos los presupuestos, la financiación y las inversiones en tecnologías y soluciones de seguridad.
    7. Activos normativos: Cumplimiento de leyes, normativas y obligaciones contractuales relacionadas con la seguridad de la información, como leyes de protección de datos, normas del sector y acuerdos contractuales con clientes y socios.
- **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 cumplimientode 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 dichos acuerdos.
- **Acuerdos de niveles de servicio:** herramientas que ayudan a proveedores y clientes de un servicio determinado a alcanzar un consenso en cuanto al nivel de calidad a 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 en forma 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.
- **BYOD:** (Bring Your Own Device), del inglés **trae tu propio dispositivo**, es la política empresarial que consiste en que los empleados utilicen sus dispositivos personales para acceder a recursos de la empresa, como puede ser el correo electrónico, bases de datos o aplicaciones personales.
- **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:** Protección de los activos de información mediante el tratamiento de las amenazas a la información procesada, almacenada y/o transportada por sistemas de información interconectados.
- **Cliente:** Organización, entidad o persona que recibe un producto y/o servicio.
- **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 delas autoridades a las iniciativas de seguridad.
- **Confidencialidad:** propiedad que determina que la información no esté disponible ni sea revelada aindividuos, entidades o procesos no autorizados, la información es accesible solamente por quienesestán 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 se usa como sinónimo de salvaguarda.
- **CCOCI:** Comando Conjunto Cibernético, Unidad Militar Conjunta (Ejército, Armada y Fuerza Aérea), cuyo objetivo es prevenir, detectar, orientar, contener, decidir, responder y recuperar ante amenazas cibernéticas de la sociedad, la soberanía nacional, independencia, integridad territorial, el orden constitucional y los intereses nacionales, 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 o comprometan 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:** normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por crear una obra literaria, artística o científica, tanto publicada o que aún no se haya publicado.
- **Despersonalización/ Enmascaramiento/ Anonimización**: proceso de transformación de datos personales de manera que no sea posible identificar a un individuo específico, ya sea directa o indirectamente. En este proceso, se eliminan o modifican ciertos atributos o elementos de los datos que podrían ser utilizados para identificar a una persona.
- **Disponibilidad**: propiedad de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

ANEXO No.2

- **Dispositivos móviles**: equipo de cómputo pequeño, cuyo concepto principal es la movilidad, el cual permite almacenamiento limitado, acceso a internet y cuenta con capacidad de procesamiento.
- **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.
- **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.
- **Framework:** conjunto estandarizado de conceptos, prácticas y criterios para enfocar un tipo de problemática particular que sirve como referencia, para enfrentar y resolver nuevos problemas de índole similar.
- **Gestión del riesgo:** actividades coordinadas para dirigir y controlar una organización en relación con el riesgo. (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 digital:** Ocurrencia de una situación que pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información o la información que el sistema procesa, almacena o transmite; o que constituye una violación a las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable. (Decreto 338/2022)
- **Incidente de seguridad de la información:** Es un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen la probabilidad 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.
- **Mejora continua:** Acción permanente realizada, con el fin de aumentar la capacidad para cumplir los requisitos y optimizar el desempeño.
- **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.

ANEXO No.2

- **NTC-ISO/IEC 27001:2022:** Norma técnica elaborada para establecer, implementar, operar, rastrear, revisar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI).
- **OTIC:** Oficina de Tecnologías de la Información y las Comunicaciones.
- **PAW:** Privilege Adminstration Workstation, Las estaciones de trabajo de acceso con privilegios (PAW) proporcionan un sistema operativo dedicado para tareas confidenciales que están protegidas contra ataques de Internet y vectores de amenazas.
- **Perfiles de usuario**: grupos que concentran usuarios con necesidades de información similares y autorizaciones idénticas sobre los recursos o sistemas de información a los que se les concede acceso según las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.
- **Phishing:** Es una forma de fraude en línea en la que los estafadores intentan obtener información personal y confidencial, como nombres de usuario, contraseñas y detalles de tarjetas de crédito, haciéndose pasar por entidades de confianza. Usualmente, los estafadores envían correos electrónicos, mensajes de texto o mensajes instantáneos que parecen ser legítimos y persuaden a las personas para que revelen información sensible o hagan clic en enlaces maliciosos que redirigen a sitios web falsos diseñados para robar información. El término "phishing" es un juego de palabras que combina "fishing" (pesca) y "phreaking" (piratería telefónica).
- **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 predefinidos 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.

- **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.
- **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.
- **RAEE:** Los residuos de aparatos eléctricos y electrónicos (**RAEE**) son aquellos elementos **que** utilizamos diariamente, **como** tablets, teléfonos, computadores o electrodomésticos y **que** cuando dejan de funcionar se vuelven inservibles y pasan a ser considerados **como RAEE**.
- **Ransomware:** Es un tipo de programa maligno que cifra archivos en el dispositivo de la víctima y luego demanda un rescate a cambio de proporcionar una clave de descifrado. Una vez que los archivos están cifrados, el usuario no puede acceder a ellos hasta que pague el rescate exigido por los perpetradores del ransomware. Este rescate generalmente se solicita en forma de criptomoneda, como Bitcoin, para dificultar el rastreo de las transacciones. Los ransomware se propagan a menudo a través de correos electrónicos de phishing, descargas de software no autorizado o vulnerabilidades en sistemas operativos y aplicaciones. Una vez que infectan un sistema, pueden propagarse a través de una red, afectando no solo el dispositivo inicial, sino también otros dispositivos conectados a la misma red. El ransomware ha sido una de las formas más lucrativas de ciberataques en la última década, y los perpetradores suelen dirigirse a individuos, empresas e incluso organizaciones gubernamentales.
- **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.

ANEXO No.2

- **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.
- **SGSI - Sistema de gestión de la seguridad de la información:** 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.
- **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 un tipo de software o programas hostiles e intrusivos que pretenden infiltrarse en un computador o 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 realizar actividades remuneradas o de prestación de servicios a terceros utilizando 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.
- **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.

ANEXO No.2

- **Test de penetración**: es un ataque dirigido y controlado hacia componentes de infraestructura tecnológica para revelar malas configuraciones y vulnerabilidades explotables
- **Tratamiento del riesgo:** procesos de selección e implementación de medidas para modificar el riesgo.
- **Trazabilidad:** Capacidad para seguir la historia, la aplicación o la localización de todo aquello queestá bajo consideración.
- **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.
- **XROAD:** X-Road es un software de código abierto que permite a instituciones y organizaciones intercambiar información a través de Internet. X-Road constituye una capa de integración distribuida entre sistemas de información, que proporciona un modo estandarizado y seguro de desplegar y utilizar servicio.

## 14. CONTROL DE CAMBIOS

| VERSIÓN | FECHA | MOTIVO DE LA MODIFICACIÓN | RESPONSABLE |
|---|---|---|---|
| 3 | 06/06/2020 | Actualización de introducción, objetivo general, alcance, compromiso de la alta dirección, competencia, roles y responsabilidades, matriz de comunicaciones y partes interesadas. | Líder del proceso |
| 4 | 14/12/2021 | 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.<br>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; Concertados a través de mesas de trabajo con algunas dependencias del Ministerio.<br>Se adiciono el numeral A.19 POLÍTICA SEGURIDAD DE DATOS | Líder del proceso |
| 5 | 17/12/2024 | Actualización de lineamientos generales de tercer nivel desde A.5.1.1 hasta A.18.2.3.con los controles de la Guía 27001:2022 A.5.1. hasta A.8.34 y se separaron dentro del documento como un Anexo No1 que se denominó GUIA DE APLICACIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.<br><br>Se adiciono el Anexo No2 correspondiente a la GUIA DE USO Y | Líder del proceso |

| VERSIÓN | FECHA | MOTIVO DE LA MODIFICACIÓN | RESPONSABLE |
|---|---|---|---|
| | | ACCESO A RECURSOS DE TIC.<br><br>El documento fue presentado y aprobado en el marco del Comité institucional de Gestión y desempeño y fue aprobado según acta 3 de 2024. | |