Superservicios
Superintendencia de Servicios Públicos Domiciliarios

# MANUAL DE POLÍTICAS COMPLEMENTARIAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SIGME

**Código DE-M-004 Versión 7**
**JUNIO, 2024**

## TABLA DE CONTENIDO

## 1. OBJETIVO

Establecer los lineamientos que permitan el adecuado tratamiento de la información, en lo que respecta la preservación de su confidencialidad, integridad y disponibilidad, mediante la implementación de controles administrativos y técnicos que soportan el Sistema de Gestión de Seguridad y Privacidad de la Información en la entidad.

## 2. ALCANCE

El presente Manual es aplicable a todos los procesos de la Superservicios y a todos sus colaboradores y terceros que presten sus servicios o tengan algún tipo de relación con la entidad.

## 3. FUNDAMENTO LEGAL

- Ley 527 de 1999, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- Ley 1221 de 2008, por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
- Ley 1266 de 2008, por la cual se dictan las disposiciones generales del Habeas Data.
- Ley 1273 de 2009, por el cual se modifica el código penal, se crea un nuevo bien jurídico tutelado denominado "De la Protección de la información y de los datos".
- Ley 1437 de 2011, Capítulo IV. “Utilización de medios electrónicos en el procedimiento administrativo”. “Los procedimientos y trámites administrativos podrán realizarse a través de medios electrónicos. Para garantizar la igualdad de acceso a la administración, la autoridad deberá asegurar mecanismos suficientes y adecuados de acceso gratuito a los medios electrónicos, o permitir el uso alternativo de otros procedimientos.”
- Ley estatutaria 1581 de 2012, por el cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- Ley 1712 de 2014, por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Decreto 2573 de 2014 Por el cual se dictan los lineamientos generales de la estrategia de Gobierno en Línea.
- Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

- Decreto 1078 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1078 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia. Parte 1 - Disposiciones reglamentarias generales. Título 1 - Disposiciones generales en materia de transparencia y del derecho de acceso a la información pública nacional.
- Decreto 728 de 2017, por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
- Decreto 1008 de 2018, por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- Manual de Gobierno Digital versión 7 de 2019, implementación de la política de Gobierno Digital.
- Marco de interoperabilidad para el Gobierno Digital (2019).
- Ley 1952 de 2019, Por medio de la cual se expide el código general disciplinario se derogan la ley 734 de 2002 y algunas disposiciones de la ley 1474 de 2011, relacionadas con el derecho disciplinario.
- Resolución 1519 del 2020, sobre transparencia en el acceso a la información, accesibilidad web, seguridad digital web y datos abiertos.
- CONPES 3995 de 2019. Política nacional de confianza y seguridad digital.
- CONPES 3975 de 2019. Política nacional para la transformación digital e inteligencia artificial.
- Decreto 620 de 2020, por el cual se subroga el título 17 de la parte 2 del libro 2 del decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la ley 1437 de 2011, los literales e), j) y literal a) del parágrafo 2 del artículo 45 de la ley 1753 de 2015, el numeral 3 del artículo 147 de la ley 1955 de 2019, y el artículo 9 del decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- Decreto 681 de 2020, por el cual se adiciona el título 19 a la parte 2 del decreto 1078 de 2015, decreto único reglamentario del sector de tecnologías de la información y las comunicaciones, para establecer las reglas para implementar el artículo 154 de la ley

1955 de 2019.

- Circular 01 de 2022 del Departamento Administrativo de la Presidencia de la República. Recomendaciones de uso de servicios en la nube como medida para mitigar riesgos de seguridad digital.
- Resolución 500 de 2021, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de gobierno digital.
- Directiva 03 de 2021 de Presidencia de la República, lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
- Directiva 02 de 2022 de Presidencia de la República, reiteración de la política pública en materia de seguridad digital.
- Resolución 460 de 2022 del Ministerio de Tecnologías de la Información y las Comunicaciones. Por la cual se expide el Plan Nacional de Infraestructura de Datos y Su hoja de ruta en el desarrollo de la Política de Gobierno Digital, y se dictan los lineamientos generales para su implementación.
- Resolución 746 de 2022 del Ministerio de Tecnologías de la Información y las Comunicaciones, por la cual se fortalece el modelo de Seguridad y Privacidad de la Información y se definen lineamentos adicionales a establecidos en la Resolución No. 500 de 2021.
- Decreto Presidencial 88 de 2022. Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 Y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea.
- Decreto 255 de 2022 del Ministerio de Comercio, Industria y Turismo. Por el cual se adiciona la Sección 7 al Capítulo 25 del Título 2 de la Parte 2 del Libro 2 de/ Decreto 1074 de 2015, Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, sobre normas corporativas vinculantes para la certificación de buenas prácticas en protección de datos personales y su transferencia a terceros países.
- Decreto 338 de 2022 del Ministerio de Tecnologías de la Información y las Comunicaciones. Por el cual se adiciona el Título 21 a la Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.
- Resolución 01117 de 2022 del Ministerio de Tecnologías de la Información y las Comunicaciones. Por la cual se establecen los lineamientos de transformación digital para las estrategias de ciudades y territorios inteligentes de las entidades territoriales,

en el marco de la Política de Gobierno Digital.

- Decreto 767 de 2022 de Presidencia de la República. Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Ley 2294 de 2023. Por el cual se expide el Plan Nacional de Desarrollo 2022-2026 "Colombia Potencia Mundial de la Vida". Artículo 143. Transformación digital como motor de oportunidades e igualdad; Artículo 144. fortalecimiento del sector TIC.

## 4. DEFINICIONES

- **Activos:** Un activo de información es un elemento definible e identificable que almacena registros, datos o información en cualquier tipo de medio y que es reconocida como vital para la operación de Superservicios.

- **Áreas seguras:** edificios, oficinas o lugares en donde se produce o se realiza la custodia de información crítica, es decir, aquella calificada como información pública clasificada o pública reservada, o información sensible, es decir, aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política y las convicciones religiosas o filosóficas, entre otros.

- **Borrado seguro:** método de borrado de archivos basado en software cuya función es sobrescribir los datos con el propósito de destruir completamente todos los datos electrónicos que residen en una unidad de disco duro u otros medios de almacenamiento.

- **Cifrado:** aquello cuya escritura se desarrolla con cifras, es decir, con signos que se utilizan y solo pueden ser comprendidos por personas que tienen acceso a dicho código o clave correspondiente.

- **Código malicioso:** son programas que tienen como objetivo acceder a un sistema operativo o sistema de información sin que se detecte su presencia. Los programas podrían: robar credenciales, datos bancarios, información y secuestrar los equipos de cómputo.

- **Confidencialidad:** principio de seguridad de la información que requiere que la información sea accesible de forma única a las personas que se encuentran autorizadas.

- **Continuidad tecnológica:** capacidad de la Oficina de Tecnologías de la Información y las Comunicaciones de la entidad, OTIC, para continuar la oferta de servicios tecnológicos dentro de un periodo de tiempo aceptable a una capacidad predefinida durante una interrupción de la operación o la ocurrencia de un desastre natural.

- **Directorio activo:** es un servicio de directorio para su uso en un entorno Windows. Se trata de una estructura de base de datos que comparte información de infraestructura para localizar, proteger, administrar y organizar los recursos del equipo y de la red, como usuarios, archivos, grupos e impresoras.

- **Disponibilidad:** principio de seguridad de la información que requiere que los sistemas de información o aplicaciones se mantengan trabajando sin sufrir ninguna degradación en cuanto a accesos. Es necesario que se ofrezcan los recursos que requieran los usuarios autorizados cuando se necesiten.

- **Dispositivos móviles:** para la Superservicios los dispositivos móviles corresponden a los equipos portátiles que son de su propiedad, los cuales son asignados para algunos funcionarios, jefes de oficina o coordinadores, y aquellos equipos que no están bajo su custodia.

- **Dispositivos removibles:** son dispositivos de almacenamiento independientes de los equipos de cómputo de escritorio y portátiles de la entidad y que pueden ser transportados libremente. Entre estos dispositivos se encuentran entre otros, los discos duros portátiles y las memorias USB.

- **EDR:** Detección y respuesta de punto final- Endpoint Detection and Response, es un endpoint de respuesta de seguridad automatizado para reducir de forma proactiva la superficie de ataque, previene la infección de malware, detecta y desactiva posibles amenazas inmediatamente, y automatiza procedimientos de respuesta y corrección con manuales de estrategias personalizables en cualquier dispositivo viejo o actual con sistema operativo Windows, macOS y Linux.

- **Incidente de seguridad y privacidad de la información:** se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información, un impedimento en la operación normal de las redes, sistemas o recursos informáticos o violación a una de las Políticas Complementarias del Sistema de Gestión de Seguridad y Privacidad de la Información.

- **Información pública:** Es la agrupación ordenada de datos públicos, que permite otorgarle a los datos una utilidad y uso en determinado contexto, y que se genera a partir del desarrollo de actividades para el funcionamiento del Estado, es decir de los

registros periódicos de las actividades misionales de las entidades, o como consecuencia del ejercicio de funciones de rutina en el Estado.

- **Información pública clasificada:** es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014.
- **Información pública reservada:** es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014.
- **Infraestructura tecnológica (Recursos tecnológicos):** es el conjunto de hardware, software y telecomunicaciones que posee la entidad junto con sus herramientas de gestión, para soportar y apoyar todas las operaciones que están a cargo de la Oficina de Tecnologías de la Información y las Comunicaciones, OTIC.
- **Infraestructura computacional:** Dispositivos de hardware con sistemas operativos y periféricos.
- **Integridad:** principio de seguridad de la información que requiere que la información se mantenga inalterada ante incidentes o intentos maliciosos y sólo puede ser modificada mediante autorización.
- **Interrupción baja:** es la materialización de una amenaza de tipo físico y/o lógico en cualquiera de los sistemas de información, aplicación y/o herramientas críticas informáticas en la entidad.
- **Jefe Autorizador**: funcionario de la SSPD con rol de Superintendente / secretaria general / Jefe de Oficina /Superintendente Delegado / Director / Coordinador
- **Portal cautivo:** formulario dispuesto para el acceso a la red Wifi – Invitado con el objetivo de poder acceder a esta red inalámbrica.
- **Redes privadas virtuales (Virtual Private Network):** es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet. La Superservicios utiliza estas redes para que sus funcionarios puedan conectarse a la intranet y a los diferentes sistemas de información de manera remota.

- **Repositorio:** es un sitio donde se almacena y mantiene información digital de la entidad y se consideran repositorios oficiales: el servidor de archivos (file server), Google Drive y los sistemas de información

- **Sistema de información:** un sistema de información es un conjunto de datos que interactúan entre sí, que ayudan a administrar, recolectar, recuperar, procesar, almacenar y distribuir información relevante para el cumplimiento de objetivos estratégicos de la entidad y los objetivos de sus procesos.

- **Teletrabajo:** forma de organización laboral que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de información y comunicación para el contacto entre el trabajador y la entidad, sin requerirse la presencia física del trabajador en sitio específico de trabajo (según la Ley 1221 de 2008 y el Decreto reglamentario 0884 de 2012.

- **Token:** dispositivo físico donde se almacena el certificado digital de función pública del usuario, para poder interactuar con el aplicativo SIIF Nación.

- **Wifi – Libre:** red inalámbrica de acceso público a internet dispuesta por la entidad para el fortalecimiento del modelo de Gobierno Digital, de acuerdo con el Decreto 728 de 2017. Este servicio funciona en territoriales y en la sede de la Calle 84.

- **Wifi – Invitados:** red inalámbrica de acceso a internet dispuesta por la entidad para las personas que llegan a las sedes de la entidad como invitados de alguno de los colaboradores de la entidad.

- **Wifi – SSPD:** red inalámbrica dispuesta por la entidad para proveer el servicio de internet a los colaboradores de la entidad.

## 5. CONTENIDO

### 5.1. POLÍTICA SEGURIDAD RECURSOS HUMANOS

**Objetivo:** Sensibilizar e informar de forma continua a los colaboradores sobre las políticas que afectan el desarrollo de sus funciones y de sus responsabilidades en materia de seguridad y privacidad de la información.

a. Antes del ingreso de los colaboradores a la Superservicios, tanto el grupo de contratos y adquisiciones como el grupo de administración de personal, deben asegurar durante el proceso de selección, la implementación de un mecanismo de verificación de antecedentes ajustado a la ley.
b. Durante el ingreso de los colaboradores a la Superservicios, tanto el grupo de

contratos y adquisiciones como el grupo de administración de personal, deben asegurar el diligenciamiento de la documentación relacionada con el tratamiento de datos personales y de seguridad de la información.

c. El Oficial de Seguridad de la Información, a cargo de la Jefa de la Oficina Asesora de Planeación e Innovación Institucional, OAPII, es el responsable de implementar todo el tema de apropiación y sensibilización en los temas de seguridad y privacidad de la información para todos colaboradores, a través de los canales institucionales establecidos.
d. Los líderes de los procesos deben reportar las novedades del personal a su cargo y los sistemas de información o aplicaciones involucrados a la Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, a través de la documentación correspondiente, que permita dar el cumplimiento con la gestión de usuarios y la correspondiente devolución de los activos que tenían a su cargo (dispositivo móvil, equipo de cómputo y carné, entre otros).

### 5.2. POLÍTICA USO ACEPTABLE ACTIVOS INFORMACIÓN

**Objetivo**: Definir las reglas necesarias para realizar la identificación de los activos de información.

a. Los activos de información son reconocidos como valiosos por cada líder de proceso y debe asegurar la designación de los propietarios de los activos de información al momento de su creación.
b. El líder de proceso debe mantener actualizado el inventario de los activos de información involucrados en el desarrollo de sus actividades.
c. El Oficial de Seguridad de la Información, liderará el ejercicio de actualización del registro de activos de información y del índice de información clasificada y reservada, y se realizará al menos una vez cada dos (2) años.
d. Los líderes de proceso y los propietarios de los activos de información deben utilizar los repositorios oficiales establecidos por la entidad, con el fin de mantener la confidencialidad, integridad y disponibilidad de estos.

### 5.3. POLÍTICA CLASIFICACIÓN Y MANEJO INFORMACIÓN

**Objetivo:** Establecer la normativa que le permita a los usuarios conocer qué medidas de protección mínimas aplica para la clasificación y manejo de la información.

a. Los líderes de los procesos deben cumplir con los mecanismos y procedimientos establecidos en la entidad para la adecuada clasificación, calificación, manejo y tratamiento de los activos de información, de acuerdo con la Ley 1712 de 2014 y la documentación establecida por la entidad para tal fin.

b. Los líderes de los procesos deben cumplir con los mecanismos y procedimientos definidos para la eliminación o destrucción de los activos de información.
c. Los líderes de los procesos deben validar de manera periódica las restricciones y clasificaciones de acceso a los activos de información críticos, de acuerdo con la política de control de acceso y uso de contraseñas.
d. Los líderes de los procesos, en el caso de que se requiera, deben gestionar la creación de Unidades Compartidas en el DRIVE para el manejo de la información relacionada con las evidencias de los planes de acción a su cargo, así como las de los contratistas para el cumplimiento de los informes de actividades.

## 5.4. POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

**Objetivo:** Evitar accesos físicos no autorizados a las instalaciones de la Superservicios, para que la información de la entidad no se vea afectada en su confidencialidad, integridad o disponibilidad.

a. Mientras permanezcan en las instalaciones de la entidad, todas las personas deben portar en lugar visible su identificación como visitante o carné que lo acredite como funcionario o contratista.
b. Los visitantes deben permanecer acompañados de un funcionario, contratista o personal de vigilancia privada, cuando se encuentren en las oficinas o áreas donde se maneje información de la entidad.
c. Es responsabilidad de todos los funcionarios y contratistas de la Superservicios, borrar la información escrita en los tableros o pizarras de las oficinas o salas de la entidad al finalizar las reuniones de trabajo; igualmente, no se deben dejar documentos o notas escritas sobre las mesas al finalizar dichas reuniones.
d. El horario autorizado para recibir visitantes en las instalaciones de la Superservicios estará sujeto a los lineamientos establecidos por Secretaría General.
e. El ingreso de funcionarios, contratistas y visitantes durante los fines de semana y días festivos debe ser reportado con mínimo 24 horas de anterioridad. La respectiva solicitud deberá realizarse con el visto bueno del jefe inmediato, dentro del horario laboral (7:00 a.m. a 4:00 p.m.), por correo electrónico, indicando los datos completos y horario de autorización, y en el caso de requerir ingreso de terceros sustentando la necesidad de autorizar el ingreso en el horario y día no laboral, recordando que para la Sede 84 y CIVIS en Bogotá deberá dirigirse a la Dirección Administrativa a través de la Coordinación del Grupo de Servicios Administrativos y a Nivel Nacional al Director Territorial respectivo..
f. Los dispositivos removibles de propiedad de la Superservicios, así como toda información clasificada y reservada de la Superservicios, independiente del medio en que se encuentre, deben permanecer protegidos permanentemente.

g. La Superservicios cuenta con cámaras de video vigilancia, con el fin de preservar la seguridad de sus colaboradores, así como monitorear y registrar las actividades realizadas dentro de sus instalaciones.
h. Las áreas seguras, dentro de las cuales se encuentran el centro de cómputo, centros de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia, cuentan con mecanismos de protección física y ambiental; además de controles de acceso adecuados para la protección de la información.
i. En las áreas seguras establecidas en la Superservicios, en ninguna circunstancia se puede fumar, consumir alimentos ni bebidas.
j. El personal de limpieza debe tener precauciones durante el proceso de aseo y se prohíbe el ingreso de maletas, bolsos u otros objetos que no sean pertinentes para esta actividad.
k. La plataforma tecnológica (Hardware, software y comunicaciones) debe contar con las medidas de protección física y eléctrica, con el fin de evitar daños, fraudes, interceptación de la información o accesos no autorizados.
l. Solo el personal autorizado por la Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, puede realizar conexiones y desconexiones de los equipos de la entidad que se encuentran en la red regulada.
m. Los equipos de cómputo propiedad de funcionarios, contratistas o visitantes que ingresen o sean retirados de la entidad, deben ser registrados por el personal de vigilancia privada en la bitácora respectiva.
n. La salida de cualquier equipo de la Superservicios se debe realizar con el formato GA-F-008 Solicitud salida de bienes de la entidad, para la autorización de salida de equipos debidamente diligenciado y firmado.

## 5.5. POLÍTICA SOBRE EL USO DE CONTROLES Y LLAVES CRIPTOGRÁFICAS

**Objetivo:** Utilizar técnicas de cifrado para la protección de la confidencialidad e integridad de los sistemas de información misionales de la entidad.

a. Las contraseñas o claves de usuarios de los sistemas de información no podrán ser almacenadas en texto plano y deberán hacer uso de mecanismos de cifrado.
b. Todos los colaboradores de la entidad que utilizan el Sistema de Información del SIIF NACIÓN para desempeñar sus funciones, deben cumplir con las políticas de seguridad de la información del SIIF Nación, expedidas por el Ministerio de Hacienda y Crédito Público (Decreto No 1068 de 2015, Parte 9, Titulo 1, Capítulo 1), relacionadas con responsabilidades de los usuarios, uso de tokens y firmas digitales, entre otros.
c. Los colaboradores de la Superservicios deben aplicar los controles necesarios para evitar accesos no autorizados a las llaves cifradas asignadas (tokens).
d. Los responsables de las llaves cifradas (tokens), deberán almacenarlas de forma

segura para evitar accesos no autorizados a las mismas.

e. El cambio o actualización de las llaves cifradas deberá ser solicitado por el personal responsable del SIIF de la entidad.
f. Se deben utilizar técnicas criptográficas para autenticar usuarios y otras entidades. El sistema debe utilizar técnicas de cifrado para proteger las contraseñas de acceso tanto en tránsito como en almacenamiento.
g. Los canales de datos, redes MPLS deberán contar con controles de cifrado de extremo a extremo con el fin de mitigar riesgos de interceptación en las comunicaciones.
h. Los sitios web de la Entidad deberán contar con certificados SSL vigentes generados por medio de un ente certificador.
i. La OTIC, deberá administrar, gestionar y custodiar los certificados digitales para la protección con cifrado de los sitios web propios de la entidad.
j. Los equipos de cómputo (portátil) de la Entidad, deberán contar con un proceso de cifrado en el disco duro, con el fin de proteger la información almacenada.
k. El Oficial de Seguridad de la Información junto con la OTIC deben establecer los estándares de cifrado seguro permitidos en la entidad y revisarlos anualmente.

### 5.6. POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA

**Objetivo:** Definir los lineamientos generales para mantener el escritorio y la pantalla limpia, con el fin de reducir el riesgo de acceso no autorizado, pérdida o daño de la información de la Superservicios.

a. Se debe activar el bloqueo de pantalla en el equipo de cómputo de la entidad, el cual está configurado en 5 minutos, de acuerdo con la herramienta que gestiona la OTIC. Sin embargo, cada usuario deberá garantizar que nadie pueda ingresar al equipo de cómputo durante su ausencia, bloqueando su estación de trabajo antes de alejarse del mismo.
b. Los documentos que se trabajan en la carpeta “escritorio” en los equipos que se encuentran en el dominio de la Superservicios, no podrán ser visualizados, con el objetivo de proteger la información y evitar la contaminación visual de las pantallas.
c. Se debe guardar bajo llave o mantener en un sitio de acceso restringido, los documentos en formato físico o en dispositivos removibles que contengan información calificada como clasificada o reservada.
d. Cuando los funcionarios y contratistas de la Superservicios se retiren de su sitio de trabajo o al finalizar su jornada laboral, deberán bloquear la sesión del computador, dando clic a las teclas “Windows” y “L” de manera simultánea, y guardar en un lugar seguro los documentos y dispositivos removibles que contengan información clasificada o reservada, esto aplica para los colaboradores que desempeñen sus

funciones y obligaciones de manera remota.

## 5.7. POLÍTICA DE RESPONSABILIDADES FRENTE A LA SEGURIDAD DE LA INFORMACIÓN

**Objetivo:** Definir las responsabilidades que deben tener los funcionarios y contratistas respecto de la seguridad de la información en la Superservicios.

a. Todos los funcionarios y contratistas de la Superservicios, que previamente han sido autorizados para acceder a los recursos tecnológicos y de procesamiento de información de la entidad, son responsables del cumplimiento de políticas, requisitos legales, normas técnicas, buenas prácticas y documentos propios del Sistema de Gestión de Seguridad y Privacidad de la Información de la Superservicios.
b. Es responsabilidad de funcionarios y contratistas almacenar la información y los documentos resultado de sus actividades laborales, en medios y repositorios de archivos dispuestos por la entidad, con el fin de garantizar su disponibilidad en el tiempo. Se consideran repositorios oficiales el file server, Google Drive y los sistemas de información de la entidad, los demás repositorios se encuentran bajo custodia de los usuarios.
c. Todos los funcionarios y contratistas de la Superservicios deben hacer buen uso de la información que se genera del desarrollo de sus actividades y, bajo ninguna circunstancia, podrán divulgar o compartir información reservada o clasificada, que ponga en riesgo la seguridad o el buen nombre de la entidad, ni hacer uso de ella en beneficio propio o de un tercero. Esto aplica incluso después de la terminación del vínculo laboral o contractual y debe definirse en los acuerdos de confidencialidad de la Superservicios.
d. Las violaciones a las Políticas de Seguridad de la Información establecidas por la Superservicios, comprometerán la responsabilidad del infractor y podrán generar acciones disciplinarias contra los servidores públicos involucrados o personal contratista, sin perjuicio de las acciones civiles o penales a que haya lugar.
e. Los colaboradores deben reportar de manera oportuna el incumplimiento de las políticas, procedimientos, evento o incidente relacionado con seguridad y privacidad de la información, utilizando la mesa de servicio a cargo de la Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, o reportando al oficial de seguridad de la información a cargo de la Jefa de la Oficina Asesora de Planeación e Innovación Institucional, OAPII.
f. manual de políticas complementarias del sistema de gestión de seguridad y privacidad de la información

## 5.8. POLÍTICA DE USO DE LA INFRAESTRUCTURA TECNOLÓGICA

**Objetivo:** Establecer los lineamientos relacionados con la utilización de los recursos de la infraestructura tecnológica de la Superservicios.

a. La infraestructura tecnológica de la Superservicios no será utilizada para actividades comerciales o para propósitos de entretenimiento, diversión o acceso a material no autorizado.
b. Los recursos tecnológicos deben ser utilizados de manera eficiente, evitando su uso para el almacenamiento de información personal, material no autorizado o cualquier otro tipo de información que no sea necesario para el desarrollo de las funciones, actividades y obligaciones contractuales.
c. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, podrá utilizar herramientas tecnológicas o procedimientos manuales para monitorear el uso de la infraestructura tecnológica y aquel material almacenado, publicado, enviado, recibido o creado a través de estos recursos.
d. Para el monitoreo o captura de tráfico por la red de datos, la Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, o a quien esta delegue, debe hacer uso de esta información únicamente con fines de detección y gestión de anomalías o problemas en la red.
e. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, o a quien delegue, podrá otorgar o denegar el acceso a los recursos de la infraestructura tecnológica a los usuarios que lo soliciten, según los lineamientos establecidos en el TI-I-020 INSTRUCTIVO CREACIÓN, ACTIVACIÓN Y DESACTIVACIÓN DE CUENTAS DE USUARIO
f. Los usuarios deben abstenerse de copiar software licenciado o adquirido por la Superservicios, usar herramientas portables no licenciadas para uso personal o beneficio de terceros, e instalar en los equipos de cómputo software no autorizado por la entidad; sólo el personal de la Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, está autorizado a realizar tales instalaciones, incluso en servidores e infraestructura tecnológica de la entidad.
g. Los usuarios deben abstenerse de introducir software malicioso en la infraestructura tecnológica de la Superservicios, así como monitorear, capturar, manipular o destruir la información que circula por la red de datos o voz.
h. Para efectos de calidad del servicio, la Oficina de Tecnologías de Información y Comunicaciones, OTIC, está facultada en el evento en que se requiera para grabar las conversaciones direccionadas, a la extensión 4500, a través de la mesa de servicio.
i. No se permite la manipulación interna o externa de cualquier equipo de la infraestructura tecnológica, por personas no autorizadas por la Superservicios.
j. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, o a quien

esta delegue, podrá realizar en cualquier momento una inspección a nivel de redes o a nivel del software instalado en los equipos de cómputo de la entidad.

k. En ningún caso, los usuarios utilizarán las herramientas tecnológicas suministradas por la entidad para cometer actos ilícitos.

l. Los usuarios deben abstenerse de conectar dispositivos activos de red, o cualquier otro hardware, a la red de datos o voz sin la autorización de la Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, o a quien esta delegue la administración de la red de la Superservicios.

m. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, o a quien delegue, debe cambiar todas las claves de acceso que vienen predeterminadas en la infraestructura tecnológica del fabricante, adquirida por la Superservicios.

n. Las contraseñas de acceso a los servidores y administración de los Sistemas de Información de la Superservicios deben ser cambiadas mínimo cada 6 meses por la Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, o a quien delegue.

o. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, o a quien esta delegue, debe realizar la sincronización automática de la hora, en los distintos servidores y demás elementos de la infraestructura tecnológica, con la hora de los servidores de la Superintendencia de Industria y Comercio (SIC) o de la entidad que registre la hora oficial para Colombia.

p. Se prohíbe el uso de la infraestructura tecnológica de la entidad para cualquier tipo de actuación que vaya en contra de la ley y normatividad vigente.

q. Ninguna dependencia de la entidad está autorizada para instalar equipos de cómputo, servidores, redes o cualquier otro componente tecnológico dentro de las instalaciones de la entidad, esta actividad es responsabilidad única de la Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, o a quien esta delegue.

r. Los usuarios deben utilizar las herramientas tecnológicas institucionales o licenciadas o aprobadas por la Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, y deben abstenerse de utilizar aquellas aplicaciones que no hayan sido explícitamente aprobadas.

**5.8.1.** Registro de eventos:

a. Determinar los eventos definidos por la Oficina de Tecnologías de la Información y Comunicaciones, OTIC, en la plataforma tecnológica que generarán un registro de auditoria de los sistemas y equipos de la Superservicios.

b. Conservar y revisar regularmente los registros (Logs) de las actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

**5.8.2.** Protección de la información de registro:

a. Asegurar que los registros de auditoría sean archivados en lo posible en un equipo diferente al que los genera.

**5.8.3.** Gestión de la vulnerabilidad técnica:

a. La OTIC, deberá contar con los recursos humanos, tecnológicos y financieros necesarios, con el fin de realizar análisis de seguridad de la información controlada, por medio de ejercicios de hacking ético y pruebas de caja blanca y gris.

b. Cada 3 meses presentar al OSI el informe sobre el estado de las vulnerabilidades para los activos críticos de hardware y software, quien hará el seguimiento respectivo.

c. Garantizar que las labores de tratamiento de las vulnerabilidades deben gestarse en coherencia con los lineamientos de gestión de cambios de TI descritos en el documento TI-M-002 MANUAL DE SERVICIOS TECNOLÓGICOS.

**5.8.4.** Gestión y monitoreo

a. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, o quien ésta delegue, deberá realizar monitoreo permanente a la infraestructura tecnológica de la Entidad con el fin de detectar comportamientos anómalos y posibles incidentes de seguridad de la información.

b. El monitoreo deberá incluir como mínimo el comportamiento del tráfico de red, sistemas de información, registros de las soluciones de seguridad perimetral, uso de recursos y control de acceso.

## 5.9. POLÍTICA DE USO DE LA RED

**Objetivo:** Definir las responsabilidades de funcionarios y contratistas de la Superservicios frente a la utilización de los servicios de red. y conectividad a internet.

a. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, o quien esta delegue, será responsable de garantizar que los puertos físicos y lógicos de diagnósticos y configuración de plataformas que soporten sistemas de información estén siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.
b. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, o quien esta

delegue, debe asegurar que la red de “Winvitados” no tenga conexión directa a los servidores a fin de evitar afectaciones a la seguridad de la información.

c. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, o quien esta delegue deberá definir un esquema de separación de las redes y de los dominios lógicos, teniendo en cuenta los servicios de información, usuarios, aplicaciones y las especificaciones dadas por los líderes de la información, siempre en cumplimiento de la Políticas de Control de Acceso, Uso Aceptable de los Activos de información y los principios de construcción de Sistemas Seguros.
d. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, o quien esta delegue será responsable de verificar que se utilicen arquitecturas de enrutamiento que limiten el acceso remoto a los puntos críticos de la red. Los controles de direccionamiento de red deberán utilizar técnicas de verificación para establecer correctamente las direcciones fuente y destino.

### 5.10. POLÍTICA DE USO DE INTERNET

**Objetivo:** Definir las responsabilidades de funcionarios y contratistas de la Superservicios frente a la utilización de los servicios de internet.

a. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, o quien esta delegue, podrá controlar o limitar el acceso a páginas web, servicios de carga y descarga de cualquier tipo de información, acceso a material multimedia en línea y material no autorizado, cuando su uso no esté sustentado en la necesidad del desarrollo de la labor, función o actividad contratada o convenida. Las excepciones deben ser justificadas por los jefes de dependencia o coordinadores de grupos internos de trabajo, a través de la HGSTI, indicando el detalle de lo necesitado y autorizado posteriormente por el Oficial de Seguridad de la Información.
b. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, o quien esta delegue, implementa los controles necesarios para la protección en la navegación hacia internet por medio de creación de perfiles y serán definidos de acuerdo con lo establecido en el Lineamiento de navegación web. Los accesos se otorgan de acuerdo con el cumplimiento de las funciones, obligaciones y/o cargo de los funcionarios o contratistas con la entidad. Lo anterior, con el fin de mitigar los riesgos inherentes al uso de internet, que incrementan los riesgos y vulnerabilidades de la información.
c. La descarga de archivos provenientes de Internet implica un riesgo para la seguridad de la información por lo cual se solicita que únicamente se haga cuando sea necesario; está prohibido la descarga de archivos con extensiones de tipo .exe, .bat, .prg, .bak, pig, entre otros.
d. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, o quien esta delegue, junto con el apoyo del oficial de seguridad de la información verifican y

emiten concepto sobre la viabilidad o no de habilitar las páginas, servicios o aplicativos webs que se encuentren bloqueados atendiendo el resultado del análisis de seguridad, dichas solicitudes deben ser realizadas a través de la HGSTI. La Entidad se reserva el derecho de suspender dichos servicios de acuerdo con situaciones de riesgo identificadas o reportadas a la Oficina de Tecnologías de Información y las Comunicaciones.

e. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC o quien esta delegue, realiza el monitoreo del origen de las conexiones al servicio de correo electrónico y VPN bloqueando las conexiones que considere sospechosas realizadas desde otros países.
f. No está autorizado el acceso, carga, descarga, copia, reproducción, almacenamiento o circulación de cualquier tipo de material de abuso sexual infantil y demás contenido no autorizado por la entidad y que esté restringido por las herramientas informáticas que posee la Superservicios. Si este comportamiento es observado o detectado, debe ser informado al líder de la dependencia correspondiente y a las autoridades pertinentes.
g. Dentro de la entidad no está permitido la utilización de dispositivos, herramientas o técnicas que permitan saltar los controles establecidos a nivel de navegación en internet.

### 5.11. POLÍTICA PARA EL TELETRABAJO Y EL ACCESO REMOTO

**Objetivo:** Establecer los requisitos necesarios para el teletrabajo de acuerdo con la definición del documento GH-M-004 Manual de Teletrabajo.

a. En caso de que la entidad provea el equipo de cómputo, de acuerdo con la disponibilidad existente, la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC, o quien delegue, lo entregará en óptimas condiciones (software licenciado y actualizado) para el desempeño de las funciones del servidor público.
b. Los servidores públicos que se acojan a la modalidad de teletrabajo deben dar cumplimiento a la resolución vigente que regula los criterios del teletrabajo en la Superintendencia de servicios públicos domiciliarios.

### 5.12. POLÍTICA PARA LA REALIZACIÓN DE TRABAJO REMOTO

**Objetivo:** Establecer los requisitos para aquellos colaboradores que trabajan sin conexión a la red interna de la Superservicios.

a. Para trabajo remoto, la entidad establece que toda la información institucional debe ser resguardada únicamente en repositorios oficiales y protegida de acuerdo con la

confidencialidad que amerite cada documento.

b. Ninguna información de carácter institucional debe estar guardada de manera local en el equipo del colaborador o en dispositivos externos.

c. Está prohibido el acceso a las herramientas ofrecidas por la entidad desde lugares públicos o a través de la utilización de redes desconocidas o inseguras.

d. Está prohibido abrir enlaces sospechosos o de fuentes desconocidas.

## 5.13. POLÍTICA DE CONTROL DE ACCESO Y USO DE CONTRASEÑAS

**Objetivo:** Definir las directrices generales para un acceso lógico controlado a la información y a los sistemas informáticos y de aplicaciones de la Superservicios.

a. Cuando se cree un usuario o se reestablezca una contraseña, la mesa de servicio de T.I. asigna una clave aleatoria y diferente para cada usuario, alfanumérica con una longitud mínima de 11 caracteres.

b. Las contraseñas son de uso personal e intransferible y es responsabilidad del usuario dar buen uso a ellas, no se permite compartirlas, divulgarlas o difundirlas y debe evitar escribirlas o dejarlas a la vista, en caso de que se presente incidente o sospecha se debe reportar a la HGSTI (mesa de servicio).

c. Si llegara a existir la necesidad de la utilización de cuentas genéricas en algún sistema de información, el líder del proceso deberá gestionar la solicitud con el Oficial de Seguridad de la Información - OSI de la entidad, quién realizará el respectivo análisis para su aprobación.

d. La Oficina de Tecnologías de la Información y las Comunicaciones - OTIC, estará a cargo de la creación, modificación e inactivación de cuentas de usuarios en los sistemas de información que tiene a su cargo, de acuerdo con las solicitudes del jefe autorizador, quien a su vez verifica periódicamente que las cuentas hayan sido creadas o desactivadas.

e. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, verifica periódicamente que las cuentas de usuario de los colaboradores que ya no laboran en la entidad y estén activas en las plataformas de apoyo de T.I. (Sistemas Operativos, Bases de Datos, Dispositivos de Comunicaciones y Dispositivos de seguridad Perimetral) sean desactivadas.

f. El acceso remoto a equipos y servidores a través de la red debe establecerse por medio de métodos de autenticación con protocolos seguros de comunicación (VPN).

g. Todos los usuarios deben dar cumplimiento a los lineamientos dados en esta política, por lo tanto, son responsables de cualquier acción que se realice utilizando el usuario y contraseña asignados.

h. El acceso a bases de datos, servidores y demás componentes tecnológicos de administración de la plataforma y sistemas de información de la Superservicios, debe estar autorizado únicamente por la Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, de acuerdo con los lineamientos establecidos por esta oficina.
i. La identificación de los usuarios (ID) de cualquier sistema deben tener asignado un responsable y permitir identificarlo plenamente.
j. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC debe realizar el mantenimiento, actualización y/o depuración de las cuentas de usuario de los sistemas de información y/o aplicativos, de acuerdo con las novedades administrativas. Además, deberán realizar la validación de las cuentas en períodos de inactividad mayores a 3 meses.

## 5.14. POLÍTICA DE ADMINISTRACIÓN DEL INVENTARIO DE LA INFRAESTRUCTURA TECNOLÓGICA

**Objetivo:** Definir las responsabilidades del Grupo de Almacén e Inventarios y la Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, frente a la asignación, control, redistribución y disposición de los equipos de cómputo adquiridos por la Superservicios.

a. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, o quien esta delegue, mantendrá actualizado el inventario de la infraestructura tecnológica de la Superservicios que se encuentre en servicio.
b. Al término de la vinculación laboral o contractual de un colaborador de la Superservicios, el líder de la dependencia o el supervisor del contrato deberá determinar si se requiere realizar la entrega en medio magnético de la información relevante del equipo de cómputo asignado, para lo cual debe solicitar el apoyo de La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, o a quien esta delegue, mediante la apertura de un caso en la herramienta de la mesa de servicio de la entidad.
c. En caso de pérdida, hurto o daño de un equipo de cómputo de propiedad de la Superservicios, se debe reportar inmediatamente a la mesa de servicio como un incidente de seguridad y seguir con lo establecido en el Manual Administración de Bienes GA-M-002.
d. Cuando un equipo de cómputo o algún dispositivo de almacenamiento sea reasignado o dado de baja, La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, o quien esta delegue, antes de entregarlo al Grupo de Almacén e Inventarios, debe ser sometido a borrado seguro de la información y del software instalado, con el fin de evitar la recuperación no autorizada de la misma.
e. Los únicos autorizados para realizar cambio de partes, actualizaciones, destapar,

desconectar, retirar, y/o reparar equipos, son los técnicos de soporte designados por la Oficina de Tecnologías de la Información y las Comunicaciones, OTIC previa solicitud a través de la mesa de servicio.

f. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC a través de la mesa de servicio, se asegura que los usuarios y perfiles de usuario que traen por defecto los sistemas operativos y software instalado en los computadores de escritorio, equipos portátiles, impresoras y demás dispositivos adquiridos por la entidad sean modificados antes de entrar en uso. Dichos elementos deben entregarse sin permisos de acceso con rol de administrador, al usuario final.

g. Ningún equipo de cómputo, información o software de la Superservicios debe ser retirado de la Superservicios sin una autorización formal.

## 5.15. POLÍTICA PARA DISPOSITIVOS MÓVILES

**Objetivo:** Proteger la información almacenada en dispositivos móviles (equipos portátiles y equipos celulares institucionales) y proporcionar las directrices para el aseguramiento de la información en aquellos dispositivos móviles que no estén bajo su custodia.

a. Se debe llevar registro de entrada y salida de los computadores portátiles que posee la Superservicios, de acuerdo con el formato GA-F-008 Solicitud salida de bienes de la entidad publicado en SIGME.

b. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, establece las redes inalámbricas autorizadas para el acceso a la información de los dispositivos móviles tanto de invitados como de los colaboradores de la entidad.

c. Todos los dispositivos móviles de propiedad de la Superservicios deben contar con un sistema de autenticación, como un código de desbloqueo o una clave.

d. Todos los dispositivos móviles donde se almacene información de la Superservicios deben tener licenciado el software que se utiliza dentro de la entidad y un software de antivirus con la base de datos de virus actualizada.

e. En caso de pérdida o hurto de un dispositivo móvil de propiedad de la Superservicios y personales, se debe hacer el denuncio ante las autoridades competentes y reportar el incidente inmediatamente al personal de la mesa de servicio por medio telefónico o colocando un caso en la Herramienta de Gestión de Tecnologías de la Información, HGSTI.

f. El uso de los dispositivos móviles institucionales es exclusivamente para realizar las labores que requiera la Superservicios.

g. No se debe almacenar información personal en los dispositivos móviles asignados por la Superservicios.

h. Ningún equipo celular debe conectarse a la red inalámbrica institucional (Wifi – SSPD).

i. Los equipos autorizados para conectarse a la red inalámbrica institucional (Wifi – SSPD) son los portátiles de propiedad de la entidad y para los portátiles de los colaboradores se debe revisar que cumplan con criterios mínimos de seguridad de la información y de derechos de utilización de software.
j. Los visitantes o invitados de los colaboradores podrán conectarse a la red de invitados (Wifi – Invitados), previo diligenciamiento de un formulario a través de un portal cautivo, en el cual se describe al colaborador que está autorizando el acceso a la red.
k. En caso de que el contratista requiera conectarse a la red inalámbrica institucional (Wifi – SSPD), el jefe o supervisor debe crear el caso en el HGSTI solicitando la autorización de la conexión del equipo portátil.
l. Es responsabilidad del contratista asegurar que el dispositivo reportado en el caso de la HGSTI sea el único que se conecte a la red inalámbrica institucional (Wifi – SSPD).

## 5.16. POLÍTICA DE USO DEL CORREO ELECTRÓNICO INSTITUCIONAL

**Objetivo:** Definir las responsabilidades de los usuarios frente al manejo del correo asignado por la Superservicios para el desempeño de sus actividades.

a. El correo electrónico institucional es utilizado por la Superservicios como un servicio tecnológico para apoyar el cumplimiento de las funciones y obligaciones de sus colaboradores y es de propiedad e interés de la entidad, por tanto, no debe ser utilizado para fines personales, de entretenimiento, diversión, ofensa, intimidación, acoso, agresión, cadenas de envío masivo no relacionadas con temas de la entidad, tendencias políticas y discriminación racial o para el envío o recepción de material no autorizado o que no tenga relación con las actividades que desempeña.
b. Es responsabilidad del usuario realizar la configuración del doble factor de autenticación (2FA) del correo electrónico institucional asignado. Los usuarios tendrán un plazo para dicha configuración, transcurrido ese plazo, la cuenta de correo quedará inactivada.
c. La Superservicios podrá realizar revisiones aleatorias a los correos electrónicos institucionales, sin que esto conlleve a un desconocimiento del derecho a la intimidad de los usuarios o algún tipo de violación relacionada, teniendo en cuenta que siendo la Superservicios una entidad pública a la luz del artículo 14 de la Ley 57 de 1985, toda información que en ella repose es pública, salvo las excepciones legales y constitucionales que se contemplen en materia de privacidad.
d. Es responsabilidad de cada usuario realizar constantemente la depuración del correo electrónico institucional mediante la opción “eliminar correo” o guardando la información en el espacio dispuesto por el servicio de almacenamiento en la Nube

que posee la entidad o de manera local en su equipo de trabajo, para lo cual el usuario podrá solicitar la asistencia a través de la mesa de servicio.

e. Todo correo electrónico que sea enviado desde el correo institucional debe llevar un pie de página cuyo contenido trate acerca de la exclusividad de la información enviada. Este mensaje debe ser generado automáticamente y debe visualizarse al final del correo.

f. El único correo electrónico autorizado para el manejo de información institucional es el asignado con el dominio @superservicios.gov.co, este cumple con los parámetros de seguridad y requerimientos de ley para tal fin.

g. Para crear grupos de correos electrónicos el jefe autorizador lo debe solicitar a través de HGSTI indicando ( nombre del grupo y el correo de los integrantes).

h. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC podrá restringir el acceso a plataformas de correo distintas a la plataforma oficial de correo institucional, con el fin de mitigar los riesgos de fuga o pérdida de información y descarga de software malicioso.

i. La Oficina de Tecnologías de la Información y las Comunicaciones, TIC se reserva el derecho de filtrar, de manera automática, los tipos de archivo que vengan anexos al correo electrónico para evitar amenazas de virus y otros programas destructivos. Todos los mensajes electrónicos serán analizados por las herramientas de protección definidas para tal fin.

j. Las cuentas de correo electrónico institucional deben ser suspendidas cuando un usuario finalice su vínculo laboral o contractual con la entidad o cuando no presenten ingreso durante más de tres meses calendarios continuos.

k. El licenciamiento asociado a la recuperación de las cuentas de los correos electrónicos institucionales de los colaboradores que se han retirado de la entidad, para temas de investigación relacionadas con aspectos disciplinarios o de control interno, está definido para los últimos 5 años.

l. Es responsabilidad del usuario informar a la mesa de servicio cuando le lleguen a su buzón correos sospechosos, cadenas y phishing, entre otros.

m. La entidad establece como Chat Corporativo la herramienta de Gmail asociado a cada correo institucional configurado. No se puede compartir información institucional por herramientas diferente a Gmail.

n. Todos los usuarios que posean acceso autorizado al Chat Corporativo, deberá mantener un adecuado, ético y responsable uso de este recurso, cuidando no dañar la imagen y reputación de la Superservicios, ni de ninguno de sus usuarios.

o. Está terminantemente prohibido el uso del Chat Corporativo para realizar cualquier otra actividad o transacciones para el desarrollo de actividades de envío de comunicaciones con la intención de difamar u ofender; así como están prohibidos mensajes, comentarios, caricaturas o chistes de carácter sexual o racial que

puedan ser considerados como hostigamiento o falta de respeto hacia otras personas. También se consideran violaciones a esta política los siguientes casos: mensajes tipo cadenas, pornografía, chistes, venta de productos o servicios, promoción a actividades que no son patrocinadas por la Entidad, y mensajes de índole político o religioso, entre otros.

p. Ninguno de los usuarios podrá utilizar el Chat Corporativo para enviar información que no sea propia del ejercicio de sus funciones y que esté enmarcada dentro de la ejecución de las mismas, como tampoco para divulgar información de carácter privado o confidencial a cargo de la Entidad, ni para dar a conocer decisiones administrativas que no se encuentren en firme y debidamente ejecutoriadas.

## 5.17. POLÍTICA DE COPIAS DE RESPALDO

**Objetivo:** Garantizar el respaldo y restauración de la información importante para la Superservicios en función de su criticidad.

a. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, o quien esta delegue recibirán por parte de los líderes de los procesos y dependencias, los requerimientos para respaldar la información en función de su criticidad y la frecuencia con que se debe realizar.

b. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, o quien esta delegue debe generar pruebas periódicas de restauración de las copias de respaldo, dándole prioridad a las aplicaciones que soporten los procesos misionales.

c. Los medios de almacenamiento con información respaldada deben ser manipulados única y exclusivamente por el personal designado por La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, para tal fin.

d. El Grupo de Gestión Documental y Correspondencia, o quien esta delegue, debe establecer los niveles de protección física y ambiental adecuados para proteger la información bajo su custodia.

e. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, o quien esta delegue, debe generar copias de respaldo de acuerdo con lo definido en el TI-I-018 Instructivo para realizar copias de respaldo de información.

f. Es responsabilidad de todos los funcionarios y contratistas almacenar la información asociada con su labor, en los repositorios oficiales establecidos por la entidad, para garantizar que la información está siendo respaldada.

g. Las copias de respaldo deben permitir identificar claramente la información que contienen, con el fin de que se facilite el proceso de restauración.

h. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, realizará

copias de respaldo según lo descrito en el documento TI-I-018 Instructivo para realizar copias de respaldo de información.

i. La solicitud para la restauración de los respaldos de información por parte de los colaboradores retirados de la Superservicios, deben realizarse mediante requerimiento formal ante la entidad, la cual será revisada y analizada por parte del líder del proceso propietario de la información y el oficial de seguridad de la información, de acuerdo con el tiempo y retención definido en el plan de backup a cargo de la Oficina de Tecnologías de la Información y las Comunicaciones.

j. Es responsabilidad de los colaboradores almacenar la información en los repositorios definidos por la Oficina de Tecnologías de Información y las Comunicaciones-OTIC y solo la información alojada en estos repositorios será respaldada.

## 5.18. POLÍTICA DE PROTECCIÓN CONTRA CÓDIGO MALICIOSO

**Objetivo:** Definir las medidas de prevención, detección y corrección frente a las amenazas causadas por códigos maliciosos a la información de la Superservicios.

a. Está restringida la ejecución de aplicaciones diferentes a las autorizadas por la Superservicios.

b. La Superservicios cuenta con un EDR para la protección a nivel de red y de estaciones de trabajo de su propiedad, contra software malicioso que provenga de descargas de sitios web de baja reputación, archivos almacenados en medios de almacenamiento removibles y contenido de correo electrónico, entre otros. Este servicio es administrado por La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, o a quien esta delegue.

c. El EDR adquirido por la Superservicios sólo debe ser instalado por los responsables de la Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, o a quien esta delegue.

d. Los equipos de terceros que son autorizados para conectarse a la red de datos de la Superservicios, deben tener un software de antivirus activo.

e. El único EDR autorizado en la Superservicios es el asignado directamente por La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, o a quien esta delegue, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para mitigar ataques de virus, spyware y otro tipo de software malicioso.

f. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, o a quien esta delegue, se reserva el derecho de monitorear las comunicaciones o la información que se generen, comuniquen, transmitan o transporten y almacenen en cualquier medio dentro de la Superservicios, en busca de virus o código

malicioso.

g. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, o a quien esta delegue, se reserva el derecho de filtrar los contenidos que se trasmitan en la red de la Superservicios, con el fin de evitar amenazas de virus.
h. Los equipos de los usuarios que se encuentren reportados por las herramientas de seguridad serán desconectados de la red Wifi.
i. La OTIC no se responsabiliza de atender fallas de hardware, software y seguridad que se presenten en los equipos que no son propiedad de la SSPD.

## 5.19. POLÍTICA DE INTERCAMBIO DE INFORMACIÓN

**Objetivo:** Asegurar la confidencialidad e integridad de la información de la Superservicios que sea transferida o intercambiada con otras entidades o partes externas.

a. El Grupo de Contratos y Adquisiciones debe incluir en los contratos, de acuerdo con sus modalidades de selección, el tema relacionado con acuerdo o compromiso de confidencialidad frente a la información que la entidad defina como información pública clasificada o información pública reservada, de igual manera, el funcionario de la Superservicios designado como Supervisor, debe verificar la aceptación y cumplimiento por parte del proveedor/contratista al mencionado compromiso.
b. Los responsables y encargados de la información deben asegurar que los datos personales que se lleguen a requerir por parte del proveedor/contratista para la ejecución del contrato, sólo podrán ser entregados a terceros, previo consentimiento de los titulares de estos, salvo en los casos que exceptúa la Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de los Datos Personales” y la normativa que la complemente.
c. Los responsables y encargados de la información deben verificar que el proceso de intercambio de información física o digital con entidades o partes externas se realice a través de los canales establecidos por la entidad y permita realizar trazabilidad del tipo de información intercambiada, el emisor y receptor de la misma y la fecha de entrega/recepción.
d. Los responsables y encargados de la información deben certificar que todo envío de información física a entidades o partes externas (documento o medio magnético), utilice únicamente los servicios de transporte o servicios de mensajería autorizados por la Superservicios, y que estos permitan ejecutar rastreo de las entregas.
e. No se debe enviar información física o digital calificada como reservada o clasificada por parte de la Superservicios a entidades o partes externas, sin conocimiento previo del jefe inmediato o el responsable de la custodia de la

información y sin las condiciones adecuadas que ayuden a la preservación de la integridad y confidencialidad de esta.

f. Los acuerdos de intercambio de información y los memorandos de entendimiento que se suscriban entre la entidad y terceras partes o proveedores, deben incluir los temas relacionados con confidencialidad y tratamiento de datos personales.

g. El Oficial de Seguridad de la Información debe velar porque la transmisión y transferencia de información de la entidad con entidades externas se realice en cumplimiento de las políticas de seguridad y privacidad de la información.

h. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC establece los estándares tecnológicos de los canales o medios autorizados para el intercambio o acceso de información en formato electrónico.

i. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC diseña e implementa los controles necesarios para proteger el intercambio o acceso de información a través de los servicios digitales (correo electrónico, VPN, USB y discos cifrados) contra interceptación, copiado, modificación, enrutado y destrucción.

j. Los intercambios o accesos de información a través de medios tecnológicos deben realizarse mediante las herramientas establecidas por la Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, así como la revisión y aprobación de los canales para el intercambio de información con la parte externa, con el fin identificar los riesgos asociados y establecer controles de seguridad si fuera posible.

k. La información compartida con externos a través de la nube autorizada por parte de la Superservicios diferente a las ofrecidas por la suit google workspace, debe ser solicitada por el jefe inmediato registrando el caso en la HGSTI. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC junto con el Oficial de seguridad establecerán el medio más seguro para compartir información, teniendo en cuenta el tiempo que estará habilitado y los controles que se deberán aplicar.

## 5.20. POLÍTICA DE DESARROLLO SEGURO

**Objetivo:** Asegurar que el software desarrollado al interior de la Superservicios o adquirido a terceras partes, cumplirá con los requisitos de seguridad y buenas prácticas establecidas para el desarrollo seguro.

a. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, debe incluir y verificar los requerimientos de Seguridad de la Información en todo el ciclo de vida del desarrollo del software.

b. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, debe realizar las pruebas pertinentes que validen y verifiquen las vulnerabilidades en la gestión de proyectos de desarrollo de software, para asegurar que las aplicaciones

de la entidad cumplen con los requerimientos de Seguridad de la Información establecidos, antes de pasar al ambiente de producción.

c. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, debe realizar pruebas funcionales a las aplicaciones de la entidad, cuando se efectúen y aprueben modificaciones o ajustes en la funcionalidad de alguno de ellos o cuando se efectúen cambios en los recursos tecnológicos que soporta la operación de dichas aplicaciones.

d. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, debe implantar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas por los líderes de los procesos correspondientes y cumplen con los requisitos de Seguridad de la Información estipulados.

e. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, debe restringir el acceso a los repositorios de códigos fuentes de las aplicaciones y debe controlar las versiones de los sistemas de información de la Superservicios, para asegurar buenas prácticas en la administración de los cambios propuestos y aprobados.

f. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, debe asegurase que los sistemas de información adquiridos o desarrollados por contratistas cuenten con un acuerdo de licenciamiento, el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.

g. Todos los desarrolladores internos o externos, contratados por la Superservicios, deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el diseño hasta la puesta en marcha.

h. Todos los desarrolladores internos o externos, contratados por la Superservicios, deben utilizar controles de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas; de igual manera, deben suministrar opciones de desconexión o cierre de sesión de los aplicativos (logout), que permitan terminar completamente con la sesión o conexión asociada.

i. No se deben realizar pruebas, instalaciones o desarrollos de software, directamente sobre el entorno de producción. Esto puede conducir a fraude o inserción de código malicioso.

j. En los ambientes de desarrollo y pruebas no se deben utilizar datos reales del ambiente de producción.

k. Los desarrollos nuevos o sistemas de información adquiridos deben contar con pistas de auditoría que permitan como mínimo revisar los accesos (login) exitosos y fallidos, así como las creaciones y modificaciones de usuarios y permisos.

l. La OTIC será la única dependencia con la capacidad de adquirir, desarrollar o

avalar la adquisición y recepción del software de cualquier tipo, conforme a los requerimientos de las dependencias, con el fin de garantizar la conveniencia, soporte, mantenimiento y seguridad de la información de los sistemas que opera la entidad.

m. Cualquier software que opere en la Superservicios y no haya sido entregado a la OTIC, no será responsabilidad de este, no se brindará soporte y no se le salvaguardara la información.

n. La especificación de los requisitos de seguridad de la información para nuevos desarrollos y sistemas de información se deben realizar en la etapa de levantamiento de requerimientos.

o. Los contratos establecidos para el desarrollo de software por parte de contratistas de la Superservicios, deben especificar los acuerdos sobre propiedad, entrega y custodia del código fuente y sus respectivas versiones, documentación técnica y de uso del software o sistema de información, derechos de propiedad intelectual, soportes del desarrollo de las actividades establecidas en la presente política.

p. Una vez concluido el desarrollo del software o sistema de información se deben ejecutar pruebas de seguridad que permitan establecer el cumplimiento de los requisitos de seguridad identificados, la eficacia de los controles implementados para los posibles riesgos, y la búsqueda de posibles vulnerabilidades.

q. Los cambios de software se realizarán siempre en el ambiente de pruebas dispuesto por la Entidad. Una vez superada la etapa de pruebas, la Oficina de Tecnologías de la Información y las Comunicaciones, OTIC documenta y coordina el paso a producción, previa presentación y aprobación por parte del comité de control de cambios.

## 5.21. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LA RELACIÓN CON LOS PROVEEDORES

**Objetivo:** Establecer los criterios de seguridad de la información en las relaciones de la Superservicios con los proveedores, para preservar la confidencialidad e integridad de los datos que se intercambien entre las partes.

a. Los proveedores o contratistas que tengan relaciones contractuales con la Superservicios deberán firmar el “Acuerdo de Confidencialidad”, para cualquier contrato o acuerdos con terceras partes, que implique un intercambio, uso o procesamiento de información de la entidad. Estos acuerdos harán parte integral de los contratos.

b. Para el ingreso a las áreas seguras definidas por la Superservicios, los proveedores o contratistas, deben estar permanentemente identificados y cumplir

con los controles establecidos por la entidad.

c. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, o a quien esta delegue, debe verificar las condiciones de comunicación segura, cifrado y transmisión de información, desde y hacia los terceros o proveedores de servicios.
d. El supervisor de contrato debe monitorear periódicamente, el cumplimiento de las obligaciones del proveedor y el "Acuerdo de Confidencialidad".
e. El supervisor de contrato debe administrar los cambios en el suministro de servicios, por parte de los proveedores o terceros, manteniendo los niveles de cumplimiento de servicio y seguridad establecidos con ellos y monitoreando la aparición de nuevos riesgos.
f. Tener en cuenta el compromiso del tratamiento de datos personales diligenciado por parte de los proveedores que manejan información de la entidad calificada como información pública clasificada o información pública reservada.

### 5.22. POLÍTICA DE GESTIÓN DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

**Objetivo:** Establecer los lineamientos para identificar, analizar, valorar, dar un tratamiento adecuado y evaluar el impacto de los Incidentes reportados de seguridad y privacidad de la información en la Superservicios.

a. Todos los funcionarios y contratistas tienen la responsabilidad de reportar, de forma inmediata los eventos, incidentes o debilidades en cuanto a la seguridad y privacidad de la información que identifiquen o se presenten, a través de la Herramienta de Gestión de Servicios de TI, HGSTI.
b. Tratar adecuadamente todos los incidentes de seguridad y privacidad de la información reportada.
c. Establecer roles y las responsabilidades en la Gestión de Incidentes de Seguridad y Privacidad de la Información.
d. Definir el instructivo de atención de Incidentes de Seguridad y Privacidad de la Información de la Superservicios.
e. Llevar una bitácora de los Incidentes de Seguridad y Privacidad de la Información reportados y atendidos.
f. Reportar y recolectar las evidencias para los entes de Gobierno pertinentes (Centro Cibernético Policial, Fiscalía, ColCert, MINTIC o Superintendencia de Industria y Comercio) y demás entidades de control cuando sean necesarias, lo más pronto posible después del Incidente.
g. Escalar los Incidentes a niveles superiores en caso de que sea requerido.
h. Hacer evaluaciones de los Incidentes presentados ya que se puede necesitar de controles adicionales.
i. Documentar todos los Incidentes de Seguridad y Privacidad reportados.

j. Realizar sensibilización a todos los usuarios sobre Incidentes de Seguridad y Privacidad de la Información.
k. Se mantendrá el registro de lecciones aprendidas de los incidentes de seguridad de la información, que sirva de insumo para el tratamiento adecuado y oportuno de nuevos incidentes de seguridad de la información.
l. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC implementa las herramientas tecnológicas necesarias para monitorear y prevenir la ocurrencia de incidentes de seguridad de la información.
m. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC podrá solicitar apoyo de entidades externas y/o proveedores para la aplicación de medidas de contención y recuperación de los activos de información afectados, previa evaluación y/o análisis del incidente.

## 5.23. POLÍTICA DE GESTIÓN DE LA CONTINUIDAD TECNOLÓGICA

**Objetivo:** Garantizar que los planes de continuidad tecnológica se ejecuten de forma segura sin exponer la información de la Superservicios.

a. La Oficina de Tecnologías de la Información y las Comunicaciones, OTIC, debe establecer los requisitos necesarios de seguridad de la información y la continuidad tecnológica en caso de situaciones adversas, como incidentes que afecten la normal operación de los sistemas de información o desastres naturales, teniendo en cuenta las necesidades de las diferentes dependencias de la entidad.
b. Cada vez que la entidad implemente nuevas soluciones de tecnología de información, se deben incluir en el plan de continuidad
c. Responder de manera efectiva ante eventos catastróficos según la magnitud y el grado de afectación de estos, manteniendo la seguridad de la información durante dichos eventos.
d. Mantener los canales de comunicación adecuados hacia los colaboradores, proveedores y demás partes interesadas.
e. La Superservicios por medio de la Oficina de Tecnologías de la información y las Comunicaciones, OTIC deberá elaborar un plan de recuperación de desastres tecnológicos para los sistemas de información críticos, de acuerdo con el análisis de impacto de negocio.
f. Se deberán definir y realizar pruebas al plan de recuperación de desastres tecnológicos, estas deberán ejecutarse de manera que simule las condiciones de un evento de indisponibilidad, sin que esto afecte la operación de los servicios.

## 5.24. POLÍTICA PARA LA GESTIÓN DE DERECHOS DE ACCESO PRIVILEGIADO

**Objetivo:** Garantizar que las cuentas privilegiadas se administren y gestionen de manera segura y no afecten la confidencialidad, integridad y de la información.

a. La cuenta configurada por defecto con rol de administrador en los sistemas de información debe ser renombrada y el nuevo nombre no debe hacer referencia a las características de la cuenta, salvo en casos donde esto no sea técnicamente posible.
b. La OTIC tendrá un listado actualizado con las cuentas que administren los recursos tecnológicos, servicios de red y sistemas de información de la entidad, con el fin de retirarlos, reasignarlos o revalidarlos.
c. Los usuarios que manejen cuentas privilegiadas deben poseer dos cuentas distintas, una para las funciones de administración y otra para las demás tareas. Se debe usar la cuenta con privilegios de administrador, sólo cuando se deba realizar actividades que requieran dichos privilegios.
d. Para las cuentas de usuario privilegiado o similares, en sistemas e infraestructura tecnológica, deberán definirse los requisitos para la caducidad de los derechos de acceso privilegiado.
e. Las pistas de auditoría se deben proteger para evitar su borrado o modificación por parte de los usuarios privilegiados monitoreados o usuarios no autorizados.
f. Cada cuatro meses la OTIC genera registros de auditoría que contengan eventos relacionados de seguridad, teniendo en cuenta criterios tales como nombre del evento, fechas y hora del evento y tipo de modificación sobre el objeto. Se deberá realizar un respaldo de esta información facilitando la revisión y el análisis de estos.

## 5.25. POLÍTICA USO DE PUERTOS USB

**Objetivo:** Crear la cultura en la SSPD el uso correcto de los puertos USB para la conexión de los dispositivos periféricos, que permiten administrar e interactuar con las herramientas del sistema operativo de los computadores de la entidad.

a. Los puertos USB de la infraestructura computacional serán utilizados para conectar solamente los dispositivos periféricos propios de los computadores, como los mouse, teclados, scanner, ticketeras, lectores de código de barras, impresora de carnets.
b. El uso de dispositivos de almacenamiento externo propiedad de los usuarios, están prohibidos para uso dentro de la infraestructura computacional de la entidad.
c. Las unidades de montaje en los sistemas operativos para almacenamiento externo en los equipos de la entidad se encuentran deshabilitados, para evitar incidentes de ciberseguridad que puedan vulnerar la información de la entidad.
d. La solicitud de autorización de uso de dispositivos de almacenamiento externos se realiza a través de HGSTI, las cuales serán revisadas por el oficial de seguridad quien

determinará la aprobación o no de la solicitud, el uso de estos dispositivos será de manera temporal.

e. El oficial de seguridad a través de la HGSTI aprueba el uso de los dispositivos de almacenamiento externo los cuales serán revisados por el EDR (Endpoint Detection and Response) y el antivirus de la entidad, para garantizar que no tenga malware o elementos maliciosos.
f. El personal de mesa de servicio asegurará que los dispositivos de almacenamiento externos aprobados estén revisados con el EDR y el antivirus para evitar la infección y propagación de malware en los equipos de la entidad.
g. El personal de mesa de servicios es el único autorizado para utilizar dispositivos de almacenamiento externo, por las actividades de soporte técnico como lo son, las realizaciones de backups de información o reparaciones de sistema operativo.
h. Los usuarios deben abstenerse de utilizar medios de almacenamiento externo para transportar información de la entidad.

### 5.26. POLÍTICA OPERACIONAL

El incumplimiento o falta a cualquiera de las políticas antes enunciadas por parte de los funcionarios y contratistas, generará acciones de tipo disciplinario, administrativo, civiles o penales según la gravedad de la misma. Estas se pondrán en conocimiento de la dependencia competente en materia disciplinaria para el caso de funcionarios y con el contratista ante las autoridades competentes.

## 6. ANEXOS

No aplica