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 2
SEPTIEMBRE, 2021

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 734 de 2002, Código Disciplinario Único.
- 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 estatutaria 1581 de 2012, por el cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 1008 de 2018, por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto número 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- Ley 1221 de 2008, por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
- 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 Por el cual se dictan los lineamientos generales de la estrategia de Gobierno en Línea.
- 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 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.
- Manual de Gobierno Digital versión 7 de 2019, implementación de la política de Gobierno Digital.
- Marco de interoperabilidad para el Gobierno Digital (2019).
- Resolución 1519 del 2020, sobre transparencia en el acceso a la información, accesibilidad web, seguridad digital web y datos abiertos.
- 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.
- 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.

4. DEFINICIONES

- **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 Informática de la entidad 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.

- **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 Informática.

- **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.

- **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 file server y los sistemas de información, los demás repositorios se encuentran bajo custodia de los usuarios.

- **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 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 por el jefe de dependencia, supervisor o jefe de recursos físicos, a través de una solicitud vía correo electrónico a la Coordinación del Grupo de Servicios Administrativos o a los directores de cada una de las Sedes Territoriales, informando número de identificación, nombre completo, dependencia y razón del ingreso. Quienes no estén relacionados en las listas entregadas al servicio de vigilancia, no podrán ingresar a las instalaciones.
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 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.

5.2. 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. 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.

5.3. 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.
b. Los documentos que se trabajan en la carpeta “escritorio” en los equipos que se encuentran en el domino 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 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.

5.4. 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 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.

5.5. 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 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, 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, 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 para tal fin.
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 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 Informática 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, 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 o a quien esta delegue la administración de la red de la Superservicios.
m. La Oficina de Tecnologías de la Información y las Comunicaciones, 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 o a quien delegue.
o. La Oficina de Tecnologías de la Información y las Comunicaciones, 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 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, y deben abstenerse de utilizar aquellas aplicaciones que no hayan sido explícitamente aprobadas.

5.6. 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, 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 mesa de servicio (Intranet o vía telefónica Ext. 4500), indicando el detalle de lo necesitado y autorizado posteriormente por el Oficial de Seguridad de la Información.
b. 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.
c. 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.

5.7. 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. Los funcionarios bajo la modalidad de teletrabajo que requieran realizar conexión remota a la red de comunicaciones interna de la entidad, deben contar con las aprobaciones requeridas para establecer dicha conexión y acatar las condiciones de uso establecidas para dichas conexiones.
b. La Oficina de Tecnologías de la Información y las Comunicaciones, o quien delegue, debe verificar los criterios tecnológicos establecidos para los funcionarios y los parámetros de seguridad de la información, para teletrabajar en la Superservicios.
c. La Oficina de Tecnologías de la Información y las Comunicaciones, o quien esta delegue, debe proveer los recursos tecnológicos necesarios para uso de esta modalidad de trabajo en la entidad, de acuerdo con la disponibilidad existente.
d. La Oficina Asesora de Planeación e Innovación Institucional (OAPII), o quien esta delegue, debe autorizar la configuración de la red privada virtual, para esta modalidad de trabajo en la entidad.

5.8. 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. La entidad establece como repositorio oficial las unidades compartidas que se definan a través de la herramienta de Google DRIVE y toda la información de trabajo debe ser resguardada en las carpetas dispuestas para tal fin, de acuerdo con la confidencialidad que amerite cada documento.
b. Ningún archivo calificado como clasificado o reservado, debe estar guardado de manera local en el equipo del colaborador.
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.

5.9. 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. asignará una clave aleatoria y diferente para cada usuario, alfanumérica con una longitud de 8 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.
c. El Oficial de Seguridad de la Información de la entidad (OSI), previo análisis, podrá autorizar el manejo de cuentas genéricas para el correo electrónico, de acuerdo con las necesidades del proceso solicitante y la definición de un único responsable por el uso de dicha cuenta.
d. La Oficina de Tecnologías de la Información y las Comunicaciones estará a cargo de la creación, modificación e inactivación de usuarios en los sistemas de información a su cargo, de acuerdo con las solicitudes de los líderes de los procesos.
e. El responsable del activo debe realizar anualmente la verificación del estado de los derechos de acceso lógico de los usuarios que terminan su contrato laboral o cambian de dependencia dentro de la entidad, y solicitar o revocar los que se encuentren activos.
f. Anualmente la Oficina de Tecnologías de la Información y las Comunicaciones verificará los

usuarios activos en las plataformas de apoyo de T.I. como son: Sistemas Operativos, Bases de Datos, Dispositivos de Comunicaciones y Dispositivos de seguridad Perimetral, y solicitará la desactivación de los que no laboren en la entidad.

g. Para las aplicaciones que así lo soporten, las contraseñas deben contener mayúsculas, minúsculas, caracteres especiales y números, con una longitud mínima de 8 caracteres, además, se mantiene un registro de las últimas 5 contraseñas utilizadas por el usuario, con el fin de evitar la reutilización de estas.
h. 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).
i. 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.
j. Reportar a la mesa de servicio sobre cualquier incidente o sospecha de que otra persona esté utilizando su contraseña o usuario asignado o que esté utilizando una contraseña y usuario que no le pertenece, para lo cual se procederá a realizar cambio inmediato de contraseña.
k. 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, de acuerdo con los lineamientos establecidos por esta oficina.
l. La asignación de usuarios a las bases de datos de Orfeo y SUI, se establecen por los roles definidos por la Oficina de Tecnologías de la Información y las Comunicaciones, y su periodicidad está sujeto a demanda.
m. Cada líder de proceso, jefe de dependencia, coordinador de grupo interno de trabajo, o supervisor de contrato es responsable de comunicar a la Oficina de Tecnologías de la Información y las Comunicaciones, el cambio de cargo, funciones o actividades o la finalización del vínculo de contratistas o funcionarios pertenecientes al proceso que lideran, para que cese el acceso a los aplicativos y equipos que tenía asignados.
n. La identificación de los usuarios (ID) de cualquier sistema deben tener asignado un responsable y permitir identificarlo plenamente.

5.10. 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 frente a la asignación, control, redistribución y disposición de los equipos de cómputo adquiridos por la Superservicios.

a. La Oficina Informática, 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 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, 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. Ningún equipo de cómputo, información o software de la Superservicios debe ser retirado de

la Superservicios sin una autorización formal.

5.11. 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. Para los dispositivos móviles de funcionarios, contratistas o visitantes que necesiten el servicio de red diferente al dispuesto por la entidad para atención al ciudadano, el líder de proceso o supervisor del contrato realizará el requerimiento a través de la herramienta de la mesa de servicio de la entidad.
c. Los dispositivos móviles de la Superservicios que estén autorizados para ser retirados de sus instalaciones deben tener cifrado el espacio en disco donde se almacena la información, para preservar la confidencialidad de la información en caso de pérdida o hurto.
d. Todos los dispositivos móviles de propiedad de la Superservicios deben contar con un sistema de autenticación, como un código de desbloqueo o una clave.
e. 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.
f. En caso de pérdida o hurto de un dispositivo móvil de propiedad de la Superservicios, 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 Aranda.
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 conectase en la red inalámbrica institucional (Wifi – SSPD) son los portátiles de propiedad de la entidad y los portátiles de los colaboradores que cumplan con las condiciones mínimas definidas por la Oficina de Tecnologías de la información y las Comunicaciones.
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.

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

5.13. 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, 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, o quien esta delegue, debe disponer y controlar la ejecución de las copias de respaldo, así como las pruebas periódicas de su restauración.
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 para tal fin.
d. La Oficina de Tecnologías de la Información y las Comunicaciones, o quien esta delegue, debe asignar los niveles de protección física y ambiental adecuados para proteger la información que se respalda.
e. El custodio externo de las cintas de respaldo debe contar con los controles de seguridad necesarios para su almacenamiento y gestión relacionada con la entrega o retiro de las mismas al responsable designado por La Oficina de Tecnologías de la Información y las Comunicaciones o a quien esta delegue.
f. Es responsabilidad de todos los funcionarios y contratistas almacenar la información crítica asociada con su labor, en el servidor de archivos establecido para tal fin, 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.

5.14. 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 antivirus 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 o a quien esta delegue.

c. El antivirus adquirido por la Superservicios sólo debe ser instalado por los responsables de La Oficina de Tecnologías de la Información y las Comunicaciones 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 servicio de antivirus autorizado en la Superservicios es el asignado directamente por La Oficina de Tecnologías de la Información y las Comunicaciones 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, 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, 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.

5.15. 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. La Oficina de Tecnologías de la Información y las Comunicaciones debe velar porque las herramientas de intercambio de información sean seguras, con el fin de proteger dicha información contra divulgación o modificaciones no autorizadas.

h. 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.

5.16. 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 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 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 de la Superservicios, 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 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 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 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. Cuando el proyecto es contratado externamente, el proveedor debe garantizar que las condiciones de seguridad descritas en esta política se cumplan en su totalidad.
j. 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.
k. En los ambientes de desarrollo y pruebas no se deben utilizar datos reales del ambiente de producción.
l. Las interfaces de los sistemas deben ser identificadas claramente para poder determinar a qué instancia se está realizando la conexión.
m. Los sistemas de información adquiridos o desarrollados por terceros deben contar con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.
n. Los sistemas de información 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.

5.17. 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, 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.

5.18. 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 mesa de servicio (Intranet o vía telefónica Ext. 4500).
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.

5.19. 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 debe establecer los requisitos necesarios de seguridad de la información y la continuidad tecnológica en caso de situaciones adversas, como desastres naturales o incidentes que afecten la normal operación de los sistemas de información, teniendo en cuenta las necesidades de las diferentes dependencias de la entidad.
b. Cada vez que se adquieran o implementen nuevas soluciones informáticas dentro de la Superservicios, se deben incluir dentro del plan de continuidad tecnológica para involucrar los controles pertinentes.
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.

5.20. POLÍTICA PARA LA GESTIÓN DE DERECHOS DE ACCESO PRIVILEGIADO

a. El responsable del activo debe solicitar al Oficial de Seguridad de la Información la aprobación para la creación de usuarios privilegiados, por ejemplo, aquellos con perfil de administrador de un sistema de información o aplicación.
b. La cuenta ‘administrador’ de 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.
c. El responsable del activo debe revisar a intervalos planificados cada seis (6) meses, los usuarios privilegiados con el fin de retirarlos, reasignarlos o revalidarlos.
d. 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.
e. Los activos de información, en la medida de lo posible, deben registrar las actividades de los usuarios privilegiados (pistas de auditoría) y los usuarios.
f. Las pistas de auditoría se deben proteger para evitar su borrado o modificación por parte de los usuarios privilegiados monitoreados o usuarios no autorizados.

6. 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.