2023

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA DE SALUD

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Las Tecnologías de la Información y las Comunicaciones son actualmente, uno de los pilares fundamentales para la prestación de los servicios de las diferentes entidades y la Secretaría Distrital de Salud no es la excepción. Bajo esa perspectiva, se puede observar que, desde la misma información gestionada y administrada, así como el equipamiento para hacer eso posible y adicionalmente a todas las labores técnicas de instalación, alteración, cambio de lugar, programación y mejoras a los sistemas de información, las tecnologías de la información y las comunicaciones están presentes.

Entendiendo lo anterior, a lo largo de este milenio, Colombia a través del Ministerio de Tecnologías de la Información y las Comunicaciones-MINTIC ha desarrollado políticas en cuanto a gobierno digital se refiere, que permiten que tanto el estado colombiano como los ciudadanos puedan trabajar sobre una base de eficiencia, transparencia y accesibilidad que se debe buscar dentro de las Entidades.

Para poder llevar a cabo esto, es necesario que desde la gestión interna de las entidades se comprenda a todo nivel la importancia de los diferentes habilitadores transversales de la política de gobierno digital en la consecución de los objetivos propuestos, donde la tecnología aporta al cumplimiento estratégico de la misionalidad de estas y es una de las fichas importantes para alcanzar la ventaja competitiva a nivel distrital y nacional.

Uno de estos habilitadores transversales, corresponde al de seguridad y privacidad de la Información, el cual busca que las entidades públicas implementen los lineamientos de seguridad y privacidad de la Información necesarios en todos sus procesos, trámites, servicios, sistemas de información, infraestructura, etc., buscando que la seguridad y privacidad de la Información sea un eje sobre el cual se armonice todo el que hacer de la Entidad y le de la fortaleza suficiente para prestar los servicios a los usuarios con la calidad, seguridad y eficiencia requeridos.

Teniendo en cuenta lo anterior, y con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de información, la alta dirección de la Secretaría Distrital de Salud (SDS), adopta la política de seguridad y privacidad de la información, estableciendo directrices generales que deben ser aplicadas por cada uno de los funcionarios y/o contratistas de la Entidad, con el propósito de mitigar los riesgos a los que día a día éstos se ven expuestos.

La presente política de seguridad y privacidad de la Información es una declaración genérica de total cumplimiento como directriz básica definida desde la alta dirección de la SDS, donde se precisan los lineamientos de seguridad y privacidad de la información definidos por la Secretaría Distrital de Salud y que está acorde al estándar ISO 27000:2013 y las directrices del Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC,

los cuales deben ser adoptados por todos los funcionarios, contratistas y terceros que tengan relación con la Entidad.

En la Secretaría Distrital de Salud, la seguridad y privacidad de la información permite realizar la identificación, valoración, aseguramiento y gestión de los activos de información además de los riesgos a los que están expuestos, en función del impacto que generado sobre para la entidad. En este sentido, se debe entender que la política de la seguridad y privacidad de la información de la SDS, hace parte de un proceso integrado por una serie de estrategias, medidas preventivas, proactivas y reactivas para proteger la información y mantener su confidencialidad, disponibilidad e integridad.

Bajo esta perspectiva, la estructuración de las pautas a partir de la Administración y Gestión del Riesgo, como fuente para identificar, analizar, controlar y mitigar los Riesgos de seguridad Digital que podrían afectar de manera negativa el logro de los objetivos estratégicos de la Entidad, es una necesidad casi imperativa, toda vez que la materialización de estos, pueden impedir la oferta adecuada, efectiva y óptima de los servicios a la ciudadanía para los cuales fue concebida la SDS.

Siendo así, la gestión de riesgos se presenta como una herramienta para el desarrollo, implementación y mejora continua de la entidad en procesos globales, estrategia y planificación, gestión, procesos de presentación de informes, políticas, valores y cultura organizacional, protegiendo el valor de la organización a partir de la seguridad y privacidad de la Información, tanto física como digital, orientada al cumplimiento normativo y a la definición de políticas que coadyuven la seguridad y privacidad de la Información.

Teniendo en cuenta lo mencionado anteriormente, las directrices definidas en esta política y pertenecientes al Sistema de Gestión de seguridad y privacidad de la Información-SGSI de la SDS como parte conformante del Modelo de Seguridad y Privacidad de la Información - MSPI , aplican a toda la entidad y son de obligatorio cumplimiento para la Alta Dirección, Subsecretarios, directores de área, Jefes de Oficina, funcionarios, contratistas, terceros, operadores y en general, a todas las personas que debido al cumplimento de sus funciones y de la SDS accedan a la información de la entidad.

2. OBJETIVO

Las Políticas de seguridad y privacidad de la Información tienen como objetivo principal establecer reglas sobre el uso de la información, los sistemas informáticos y de comunicaciones de la Secretaría Distrital de Salud (SDS), por parte de los usuarios, administradores o terceros, buscando la protección de los recursos de información de la Entidad y la Tecnología utilizada para su procesamiento, frente a las amenazas internas o

externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

La política de seguridad y privacidad de la Información busca establecer controles, que regulen de manera efectiva el acceso de los usuarios a los sistemas a nivel de aplicación, sistema operativo, base de datos, red y acceso físico.

3. ALCANCE

En la Secretaría Distrital de Salud la gestión de la seguridad y privacidad de la Información busca establecer y mantener programas, controles y políticas para conservar la confidencialidad, integridad y disponibilidad de la información.

El Sistema de Gestión de seguridad y privacidad de la Información debe ser aplicado a los activos de la SDS (hardware, software, servicios y documentos); así como los datos e información, sin diferenciar la presentación o formato de almacenamiento, al igual que las plataformas tecnológicas, sus procesos y procedimientos internos.

4. MARCO LEGAL Y TECNICO

A continuación, se define el marco normativo colombiano sobre el cual se fundamenta el Sistema Integrado de seguridad y privacidad de la Información. Para mayor profundidad en la normatividad dirigirse al normograma del proceso.

- **Artículo 15, Constitución Política De Colombia**: se establece que “todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, debiendo el estado respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en los archivos de Entidades públicas y privadas”.
- **Ley 23 de 1982: Ley sobre derechos de autor.**
- **Ley 1032 de 2006**: Por la cual se modifican los artículos 257, 271, 272 y 306 del Código Penal. Artículo 271. Violación a los derechos patrimoniales de autor y derechos conexos. Modificación del código Penal Colombiano Ley 599 de 2000.
- **Ley 1266 de 2008**: Por la cual se dictan las disposiciones generales del hábeas data y regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- **Ley 1273 de 2009**: Por la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado denominado "De la protección de la información y los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

- **Norma Técnica 1105 de 2011**: Instrucciones para garantizar adecuados niveles de seguridad en la elaboración, manejo, difusión, clasificación de la documentación clasificada.
- **Ley 1581 De 2012**: Por la cual se dictan disposiciones generales para la protección de datos personales tiene como objeto "(…) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales" y que dicta, además de las disposiciones generales para la protección de datos personales.
- **Decreto 1377 De 2013**: Por el cual se reglamenta parcialmente la Ley 1581 de 2012" y se dictan disposiciones generales para la protección de datos personales.
- **Norma Técnica 6 de 2013**: Actualización Directiva Permanente No. 007 de 2006, Políticas de desarrollo de software.
- **Ley 1712 De 2014**: Por la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- **Conpes 3854 de 2016**: Lineamientos y directrices de seguridad digital y se tienen en cuenta componentes como la educación, la regulación, la cooperación, la investigación, el desarrollo y la innovación.
- **Ley 1928 de 2018**: Por la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest.
- **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 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- **Conpes 3975 de 2019**: Política Nacional para la Transformación Digital e Inteligencia Artificial.
- **Conpes 3701 de 2011**: Lineamientos de políticas para la Ciber seguridad y Ciberdefensa.
- **Decreto 2106 de 2019**: Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
- **Directiva Presidencial 02 del 2 de abril de 2019**: Por la cual se establecen lineamientos de simplificación de la interacción digital entre los ciudadanos y el Estado.
- **Circular Externa Conjunta No. 04 del 5 de septiembre de 2019**: Tratamiento de datos personales en sistemas de información interoperables.
- **Conpes 3995 de 2020**: Política nacional de confianza y seguridad digital.
- **Acuerdo Distrital No. 257 de 2006:** Por el cual se define a la Secretaría Distrital de Salud es un organismo del Sector Central con autonomía administrativa y financiera.

5. ENUNCIADO DE LA POLÍTICA

La alta dirección de la Secretaría Distrital de Salud, entendiendo que la información es uno de sus activos más valiosos y de mayor importancia, se ha comprometido con la implementación, operación y mejora continua de un Sistema de Gestión de seguridad y privacidad de la Información buscando establecer un marco de confianza en el ejercicio de sus deberes con los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión, visión, estrategias y necesidades de la Entidad.

Para la Secretaría Distrital de Salud, la protección y el buen uso de la Información busca la disminución del impacto generado por amenazas y riesgos a los que está expuesta, comprometiéndonos así a mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma.

6. COMPROMISOS

Teniendo en cuenta el Acuerdo Distrital No. 257 de 2006, la Secretaría Distrital de Salud es un organismo del Sector Central con autonomía administrativa y financiera que tiene por objeto orientar y liderar la formulación, adaptación, adopción e implementación de políticas, planes, programas, proyectos y estrategias conducentes a garantizar el derecho a la salud de los habitantes del Distrito Capital. De la misma manera, según Resolución No. 842 del 04 de junio de 2021 de la SDS se crea el Comité Institucional de Gestión y Desempeño, el cual para la implementación de la dimensión de Gestión con Valores para Resultados adopta la Seguridad Digital como Política de Gestión y Desempeño Institucional y aprueba la creación de la mesa técnica de Gobierno y Seguridad Digital, la cual tiene las siguientes funciones:

- Formular las necesidades de recursos físicos y financieros para la implementación de las políticas de gestión y desempeño a su cargo, las cuales deben ser presentadas ante el Comité Institucional de Gestión y Desempeño, para su aprobación.

- Solicitar al Secretario Técnico del Comité, a través del Líder respectivo, la incorporación de los asuntos que considere pertinentes en la agenda de las sesiones.

- Establecer las herramientas, instrumentos y/o lineamientos necesarios para la aplicación de las políticas de gestión y desempeño institucional a su cargo y coordinar su respectiva articulación y gestión.

- Definir el Plan de acción y periodicidad de reuniones, para la adecuada implementación, sostenibilidad y mejora de los atributos de calidad de las políticas de gestión y desempeño institucional.

- Realizar el respectivo seguimiento al grado de avance de la implementación de las políticas de gestión y desempeño institucional y formular las acciones de mejora que permitan optimizar la eficacia, eficiencia efectividad de éstas.

- Preparar y consolidar la documentación necesaria, para el desarrollo de los temas técnicos a cargo de cada uno de los equipos o mesas técnicas.

- Desarrollar acciones de promoción, divulgación, sensibilización y/o capacitación de las herramientas, instrumentos y/o lineamientos que apoyen la implementación de las políticas de gestión y desempeño institucional a su cargo.

- Presentar los informes que le sean requeridos, por el Comité Institucional de Gestión y Desempeño o cualquier otra instancia interna o externa, sobre los asuntos a su cargo.

- Las demás que le sean asignadas en relación con el Sistema de Gestión distrital y su marco de referencia: Modelo Integrado de Planeación y Gestión — MIPG.

El Comité Institucional de Gestión y Desempeño propondrá a la autoridad que corresponda para su aprobación la definición y asignación de las responsabilidades que surjan de la presente Política.

Todo el personal de la Entidad es responsable de la implementación y cumplimiento de las Políticas de seguridad y privacidad de la Información dentro de sus dependencias.

El Comité Institucional de Gestión y Desempeño aprobará estas Políticas y son responsables de la autorización de sus modificaciones.

6.1. POLÍTICAS ESPECÍFICAS BÁSICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A continuación, se definen las políticas básicas de seguridad y privacidad de la información, las cuales deben ser conocidas y aplicadas por todos los funcionarios, contratistas y partes interesadas de la entidad.

6.1.1. ORGANIZACION DE LA SEGURIDAD

Responsabilidades Generales

a. Todo personal de la Entidad cualquiera sea su situación contractual, debe ser responsable de la seguridad y privacidad de la Información.

b. El responsable de la seguridad y privacidad de la Información será el encargado de impulsar la implementación de la presente Política.
c. El Comité Institucional de Gestión y Desempeño o quien haga sus veces tendrá a cargo el seguimiento de las actividades relativas a la seguridad y privacidad de la Información, de acuerdo con el numeral No. 1 del artículo 8 de la resolución No. 842 de junio 04 de 2021, “Aprobar y hacer seguimiento, por lo menos una vez cada tres (3) meses, de las acciones y estrategias adoptadas para la operación del Modelo Integrado de Planeación y Gestión, así como a los planes, programas, proyectos necesarios para la implementación interna de las políticas de gestión”.
d. El Director Tecnologías de la Información y las Comunicaciones – TIC como responsable de la seguridad y privacidad de la Información tendrá a cargo asesorar a los colaboradores de la SDS en materia de seguridad y privacidad de la Información y coordinará la interacción con entidades especializadas. Así mismo, junto con los propietarios de la información, analizará el riesgo de los accesos de terceros a la información de la SDS y verificará la aplicación de las medidas de seguridad necesarias para la protección de la misma.

Procesamiento de Información

a. Es responsabilidad de los Subsecretarios, Directores, Subdirectores o Jefes de Oficina, simultáneamente con el Director de la Dirección de Tecnología de la información y las Comunicaciones - TIC, autorizar o no, el uso de nuevos recursos de procesamiento de información y propender que se cumplan todas las Políticas y requerimientos de seguridad pertinentes.
b. Es responsabilidad del Director de la Dirección de Tecnología de la información y las Comunicaciones y del responsable del área al que se destinen los recursos, autorizar o no el uso de recursos personales de procesamiento de información en el lugar de trabajo, previa evaluación de cada caso por el personal de apoyo.

Asesoramiento Especializado

a. El responsable de la seguridad y privacidad de la Información será el encargado de coordinar los conocimientos y las experiencias disponibles en la entidad a fin de brindar ayuda en la toma de decisiones en materia de seguridad y privacidad de la información.
b. El responsable de la seguridad y privacidad de la Información podrá obtener asesoramiento de entidades especializadas con el objeto de optimizar su gestión en seguridad y privacidad de la Información de la SDS.
c. El responsable de la seguridad y privacidad de la Información debe garantizar que se firme un compromiso de Confidencialidad previo al intercambio de información confidencial para fines de asesoramiento o de transmisión de experiencias con aquellas

Organizaciones especializadas en temas relativos a la seguridad y privacidad de la Información, mediante formato No. SDS-TIC-FT-014 y debe ser remitido a la Dirección TIC.

Revisión independiente

a. La Oficina de Control Interno o en su defecto quien sea propuesto por el Comité Institucional de Gestión y Desempeño o quien haga sus veces debe realizar revisiones independientes sobre la vigencia e implementación de la Política de seguridad y privacidad de la Información, a efectos de garantizar que las prácticas de la SDS reflejen adecuadamente sus disposiciones y compruebe que las políticas que se definan se cumplan a cabalidad.

Acceso a la información por parte de terceros

a. El responsable de la seguridad y privacidad de la Información y el Propietario de los Activos de Información, deben llevar a cabo anualmente o cuando se requiera por motivos de cambios de contexto organizacional una evaluación de riesgo para identificar los requerimientos de controles específicos antes de otorgar acceso a terceras partes a la información de la SDS.
b. El responsable de la seguridad y privacidad de la Información y el Propietario de los activos de Información deben realizar el diligenciamiento mediante del formato No. SDS-TIC-FT-047, describiendo dicha evaluación y la decisión tomada respecto a dar acceso a terceros, debidamente firmada.

6.1.2. GESTIÓN DE ACTIVOS

Responsabilidades Generales

a. Es responsabilidad de los propietarios de la información inventariar, clasificar, documentar y mantener actualizada la información a su cargo de acuerdo con su grado de sensibilidad y criticidad, así como definir los permisos de acceso a la misma.
b. El responsable de la seguridad y privacidad de la Información debe asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.
c. El responsable del proceso de activos de información debe definir el procedimiento o lineamiento correspondiente para adelantar las actualizaciones, periodicidades, formato de reporte y demás consideraciones, de acuerdo a las necesidades de la entidad y la documentación solicitada por los entes rectores del tema.

d. El responsable del proceso de activos de información debe adelantar la capacitación y acompañamiento sobre el tema, a todos los propietarios de los activos de información.

Inventario de Activos

a. Es responsabilidad de los Subsecretarios, Directores, Jefes de Oficina y los Subdirectores identificar los activos de información asociados a cada sistema de información, sus respectivos propietarios, utilización y su ubicación.
b. Es responsabilidad de los Subsecretarios, Directores, Jefes de Oficina y los Subdirectores mantener actualizado el inventario, el cual debe ser revisado por parte del responsable de activos de información con una periodicidad no mayor a un (1) año.

Clasificación de la Información

a. Solo el Propietario de la Información, puede asignar o cambiar su nivel de clasificación, cumpliendo con los siguientes requisitos previos:
   - Asignarle una fecha de efectividad.
   - Comunicárselo al custodio del recurso.
   - Realizar los cambios necesarios para que los usuarios conozcan la nueva clasificación.
   - Justificar la nueva clasificación de acuerdo a las necesidades de la misma.
b. Es responsabilidad de los Propietarios de la información, luego de clasificarla, identificar los recursos asociados (sistemas, equipamiento, servicios, entre otros) y los perfiles funcionales que deberán tener acceso a la misma.
c. La información solo puede estar clasificada siguiendo los siguientes criterios (LEY 1712 DE 2014):
   - Pública
   - Publica clasificada
   - Publica Reservada

6.1.3. SEGURIDAD DE LOS RECURSOS HUMANOS

Responsabilidades Generales

a. El responsable de la seguridad y privacidad de la Información debe hacer el seguimiento, documentación y análisis de los incidentes de seguridad reportados y comunicar al Comité Institucional de Gestión y Desempeño o quien haga sus veces y a los propietarios de la información y de ser necesario solicitar al secretario del Comité Institucional de Gestión y Desempeño o quien haga sus veces citación extraordinaria.
b. El Comité Institucional de Gestión y Desempeño o quien haga sus veces será responsable de implementar los medios y canales necesarios para que el responsable

de la seguridad y privacidad de la Información maneje los reportes de incidentes y anomalías de los sistemas. Así mismo, dicho Comité, tomará conocimiento, efectuará el seguimiento de la investigación, controlará la evolución e impulsará la resolución de los incidentes relativos a la seguridad de la información.

c. El responsable de la Subdirección de Contratación y de Talento Humano participarán en la elaboración del Compromiso de Confidencialidad que deben firmar los funcionarios, contratistas y terceros que desarrollen funciones en la SDS.
d. Todo el personal de la SDS es responsable del reporte de debilidades e incidentes de seguridad de la información que se detecten.

Antes de asumir el empleo

a. Es responsabilidad de todos los funcionarios firmar un Compromiso de Confidencialidad y no Divulgación, en lo que respecta al tratamiento de la información de la Entidad.

Durante la ejecución del empleo

b. Es responsabilidad de la Subsecretaría Corporativa coordinar las acciones de capacitación y/o concientización en temas de seguridad y privacidad de la Información por lo menos dos veces al año.
c. Es responsabilidad y deber de cada funcionario asistir a los cursos de concientización en seguridad y privacidad de la Información que la Entidad programe y aplicar la seguridad de la información según las políticas y los procedimientos establecidos.
d. Todo el personal de la SDS debe comunicar a la mesa de ayuda los incidentes relativos a la seguridad de la información que perciba, por medio de correo electrónico, ticket de mesa de ayuda y/o vía telefónica.
e. El responsable de la seguridad y privacidad de la Información indicará los recursos necesarios para la investigación, monitoreo y resolución del incidente. Así mismo, presentara al Comité Institucional de Gestión y Desempeño o quien haga sus veces un reporte de la ocurrencia de incidentes de seguridad por lo menos una vez al año o cuando sea necesario.

6.1.4. SEGURIDAD FÍSICA Y DEL ENTORNO

Responsabilidades Generales

a. Es responsabilidad del Director de la Dirección de Tecnologías de la Información y las Comunicaciones y los propietarios de información, según corresponda, definir y controlar las medidas de seguridad física y ambiental para el resguardo de los activos de información.

b. Es responsabilidad de los Propietarios de la Información autorizar formalmente el trabajo fuera de las instalaciones con información de su interés a los funcionarios, cuando lo crean conveniente.
c. Todo el personal de la SDS es responsable del cumplimiento de la política de pantallas y escritorios limpios, para la protección de la información relativa al trabajo diario en las oficinas.
d. El responsable de la seguridad y privacidad de la Información es el encargado de revisar que el centro de procesamiento de datos y los cuartos de comunicaciones estén protegidos físicamente contra el acceso no autorizado, daño o interferencia.

Perímetro de seguridad Física

a. El responsable de la seguridad y privacidad de la Información debe definir y monitorear las medidas de seguridad de la información a implementar en áreas restringidas y controlar el mantenimiento del equipamiento informático de acuerdo con las indicaciones de los proveedores.
b. Las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica y de aire acondicionado son consideradas áreas restringidas, por lo tanto es responsabilidad del Director de la Dirección de Tecnologías de la Información y las Comunicaciones definir la fortaleza de cada barrera de seguridad para proteger esta área y de esa manera, exigir a la Subsecretaría Corporativa, la garantía de su funcionalidad y actualización por aspectos de evolución tecnológica o nuevas necesidades.

Controles de Acceso Físico

a. El responsable de la seguridad y privacidad de la información determina las áreas protegidas que se resguardarán mediante el empleo de controles de acceso físico a fin de permitir el acceso solo al personal autorizado.

Equipos Desatendidos

a. El responsable de la seguridad y privacidad de la Información debe coordinar las tareas de concientización a todos los usuarios y contratistas e incluir procedimientos de seguridad para la protección de equipos desatendidos.
b. Los usuarios son responsables de cumplir con las siguientes pautas:
   - Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ejemplo, un protector de pantalla protegido por contraseña.
   - Proteger los PC's contra usos no autorizados mediante un bloqueo de seguridad o control equivalente, por ejemplo, contraseña de acceso cuando no se utilizan.

c. No esta permitido que personas ajenas a la Entidad utilicen los computadores y/o terminales de la Entidad, si no es autorizado por el jefe inmediato del área.
d. El acceso a equipos o infraestructura ubicados en áreas restringidas, por parte de personas ajenas a la Entidad, deberán ser autorizados por el Director de la Dirección de Tecnologías de la Información y las Comunicaciones, pero no limitada a mantenimiento, soporte, inspecciones programadas, transferencia de conocimiento, reparaciones, actualizaciones, ejecución de garantías, entre otras situaciones.

6.1.5. SEGURIDAD DE LAS OPERACIONES

Responsabilidades Generales

El responsable de la seguridad y privacidad de la información debe:

a. Establecer criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, contemplando la realización de las pruebas necesarias antes de su aprobación definitiva.
b. Definir el manejo de incidentes de seguridad .
c. Definir el manejo y administración de los medios de almacenamiento.
d. Definir y documentar una guía clara con respecto al uso del correo electrónico.
e. Controlar los mecanismos de distribución y difusión de información electrónica dentro de la Entidad.
f. Definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y garantizar la seguridad de los datos y los servicios conectados en las redes de la SDS.
g. Desarrollar documentación adecuada de concientización de usuarios en materia de seguridad y privacidad de la Información.
h. Verificar el cumplimiento de las normas, procedimientos y controles establecidos.

Es responsabilidad del Director de la Dirección de Tecnologías de la Información y las Comunicaciones:

a. Controlar la existencia de documentación actualizada relacionada con las comunicaciones y operaciones.
b. Evaluar el posible impacto operativo de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación, asignando responsabilidades.
c. Administrar los medios técnicos necesarios para permitir la segregación de los ambientes de procesamiento.
d. Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad.

e. Controlar la realización de las copias de respaldo de información, así como la prueba periódica de su restauración.
f. Asegurar el registro de las actividades realizadas por el personal operativo, para su posterior revisión.
g. Desarrollar y verificar el cumplimiento de documentos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.
h. Gestionar la Implementación de los controles de seguridad definidos para el cumplimiento de los controles planteados por la ISO 27001:2013 Anexo A.
i. Definir e implementar controles sobre los documentos y la gestión de medios informáticos de almacenamiento, como cintas, discos, usb y la eliminación segura de los mismos.

Es responsabilidad de los funcionarios:

a. Reportar con diligencia, prontitud y responsabilidad presuntas violaciones de seguridad a través de su jefe de dependencia, mesa de ayuda o a la Dirección de Tecnologías de la Información y las Comunicaciones, la cual debe garantizar las herramientas informáticas para contrarrestar el incidente.

Controles Contra Software Malicioso

a. El responsable de seguridad y privacidad de la información debe definir controles de detección y prevención para la protección contra software malicioso.
b. Es responsabilidad del Director de la Dirección de Tecnologías de la Información y las Comunicaciones el gestionar la implementación de los controles contra software malicioso o solución informática equivalente.
c. Todos los equipos informáticos de proveedores o terceros que sean autorizados para conectarse a la red corporativa de la Entidad deben contar con una aplicación de antivirus con su base de datos actualizada.
d. El manejo de la aplicación de antimalware corporativo para estaciones de trabajo y servidores (instalación, configuración, administración y/o desinstalación) debe ser realizado únicamente por el personal de la Dirección de Tecnologías de la Información y las Comunicaciones o mesa de ayuda previamente capacitados para dicha actividad.

Copias de Respaldo y Restauración de la Información

a. Es responsabilidad del Director de la Dirección de Tecnologías de la Información y las Comunicaciones determinar los requerimientos para resguardar cada software y datos en función de su criticidad.
b. Es responsabilidad del Director de la Dirección de Tecnologías de la Información y las Comunicaciones disponer y hacer seguimiento a la realización de copias de respaldo de

la información, así como asegurar que se realicen pruebas periódicas de su restauración.

c. Los recursos de almacenamiento de información que destine la Dirección de Tecnologías de la Información y las Comunicaciones solo se deberán usar para alojar información propia de la Entidad y no con fines personales del usuario.
d. Es responsabilidad del Director de la Dirección de Tecnologías de la Información y las Comunicaciones definir procedimientos para la eliminación segura de los medios de información.
e. Es responsabilidad de los propietarios de activos de información el mantener depurada la información de sus archivos públicos, como buena práctica para la optimización del uso de los recursos que entrega la entidad a su personal.

Registro de Actividades y Fallas

a. Es responsabilidad del Director de la Dirección de Tecnologías de la Información y las Comunicaciones, o de quien se designe, asegurar el registro de las actividades realizadas en los sistemas, incluyendo según corresponda:
   - Errores del sistema y medidas correctivas tomadas.
   - Intentos de acceso a sistemas, recursos o información crítica o acciones restringidas
   - Ejecución de operaciones criticas
   - Cambios a información critica
b. Es responsabilidad del Director de la Dirección de Tecnologías de la Información y las Comunicaciones desarrollar y verificar el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.

6.1.6. SEGURIDAD DE LAS COMUNICACIONES

Responsabilidades Generales

a. El responsable de seguridad y privacidad de la información debe definir controles para garantizar la seguridad de los datos y los servicios conectados en las redes de la Entidad contra el acceso no autorizado.
b. Salvo expresa autorización, ningún usuario está autorizado para escanear, acceder o manipular directa o indirectamente los sistemas de información y de comunicaciones de la red de datos de la SDS, e instalar nuevos sistemas de comunicaciones de redes que se conecten con la red de datos de la Secretaría.

Correo Electrónico y almacenamiento en la nube

a. El responsable de seguridad y privacidad de la información debe definir y documentar el uso del correo electrónico que incluya los siguientes aspectos:
   - Definir el alcance del uso del correo electrónico y el almacenamiento en la nube por parte del personal de la Entidad.
   - Protección contra ataques al correo electrónico e información en la nube, por ejemplo, virus, interceptación, entre otros.
   - Protección de archivos adjuntos de correo electrónico o almacenados en la nube.
   - Controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados.
   - Aspectos operativos para garantizar el correcto funcionamiento del servicio.
   - Potestad de la Entidad, para auditar los mensajes recibidos o emitidos por los servidores de la Entidad, lo cual se incluirá en el "Compromiso de Confidencialidad".
b. Los usuarios de correo electrónico no están autorizados a enviar información en forma masiva a múltiples direcciones de correo electrónico.
c. Ningún usuario de correo electrónico debe modificar, falsificar o eliminar cualquier información que aparezca en cualquier lugar de un mensaje de correo electrónico, incluyendo el cuerpo del mensaje o encabezado.
d. Ningún empleado puede usar cuentas gratuitas de correo electrónico en internet para el envío de mensajes corporativos de la Entidad. Todos los mensajes de carácter corporativo deberán ser enviados a través del sistema de correo electrónico corporativo y designado, el cual es el único avalado para tal efecto.
e. Salvo que exista una autorización previa, ningún empleado está autorizado para interceptar, revelar o contribuir en la intercepción de mensajes de correo electrónico a través de herramientas de escaneo.
f. Los usuarios del servicio del correo electrónico de la SDS no deben contestar mensajes SPAM.
g. Ningún usuario del servicio de correo electrónico debe prestar atención a mensajes con falsos contenidos de virus, ofertas de premios, dinero, solicitudes de ayuda caritativa, venta de bienes (hardware o software) o financiamiento a muy bajo costo, productos medicinales, acceso gratuito a portales, advertencia de virus de fuentes desconocidas, entre otros.
h. Para todos los funcionarios o usuarios del servicio de correo electrónico, está prohibido brindar servicios que, de manera directa o indirecta, faciliten la proliferación de spam, en esto se incluye casillas de correo, software para realizar spam, hosting de sitios de Web para realizar SPAM o que realicen SPAM, o bien que realicen bromas de mal gusto y/o fraudes, estos últimos definidos como un correo electrónico que atrae el interés del usuario y que esconde una maniobra deshonesta y brindar servicios que, de manera directa o indirecta, faciliten la proliferación de software malicioso o malware, software espía o spyware o phishing.
i. A los usuarios que de acuerdo con sus funciones requieran una cuenta de correo, esta se les asigna una vez son vinculados. El supervisor o jefe correspondiente es el

encargado de activar el procedimiento de gestión de usuarios, sobre las vinculaciones que requieran creación de cuenta de correo; de igual manera debe informar oportunamente los retiros de los usuarios para la suspensión de este servicio. Esta cuenta estará activa durante el tiempo que dure la vinculación del usuario con la Entidad, excepto en casos de fuerza mayor o mala utilización, que eventualmente, puedan causar la suspensión o cancelación de la misma. Una vez se produzca la desvinculación o la terminación de la relación contractual de la persona, la cuenta será dada de baja mediante una solicitud enviada a la mesa de ayuda.

j. El buzón de correo es personal e intransferible y corresponde al colaborador velar por la seguridad protegiendo su clave de acceso. El usuario es el único responsable por el buen uso de su cuenta de correo electrónico.

Conexiones a Internet

a. Los ingenieros autorizados de la Dirección TIC o el operador del centro de datos, son los responsables de revisar regularmente todos los logs y archivos de auditoria de la actividad en línea de los usuarios de Internet. Esta información se considera reservada.
b. Es responsabilidad de la Dirección TIC o el operador del centro de datos evaluar e implementar las nuevas herramientas tanto de software como de hardware para que la conexión a internet sea lo más eficaz, eficiente y segura posible, ejerciendo los controles correspondientes.
c. El uso de Internet debe estar destinado exclusivamente a la ejecución de las actividades de la Entidad y deben ser utilizados por el usuario para realizar las funciones establecidas para su cargo.
d. El usuario debe abstenerse de descargar programas que realicen conexiones automáticas o visores de sitios clasificados como pornográficos o maliciosos y la utilización de los recursos para distribución o reproducción de este tipo de material, ya sea vía web o medios magnéticos.
e. La descarga de música y videos no es una práctica permitida.
f. Abstenerse de usar sitios que salten la seguridad del servidor de acceso a Internet (proxy).
g. Evitar coleccionar, almacenar, difundir, transmitir, solicitar, inducir o incitar en cualquier forma actos ilegales, inmorales, engañosos y/o fraudulentos, toda vez que es una responsabilidad de los usuarios de la Entidad, así como también amenazas, abusos, difamaciones, injurias, calumnias, escándalos, actos obscenos, pornográficos, profanos, racistas, discriminatorios, actos que invadan la privacidad de los demás u otro tipo de materias, informaciones, mensajes o comunicaciones de carácter ofensivo.

Carga y descarga de archivos

a. Los ingenieros autorizados de la Dirección TIC o el operador del centro de datos deben realizar una evaluación de virus por medio de herramientas para tal fin, a los archivos descargados o adjuntos.
b. Los usuarios deben cumplir los requerimientos de licencia y las restricciones de copia asociadas con cualquier archivo descargado u obtenido por algún medio.
c. El personal técnico de la Dirección TIC o el operador del centro de datos, únicamente instalará los archivos (ejecutables) absolutamente necesarios para las funciones de la SDS.

6.1.7. CONTROL DE ACCESO

Responsabilidades Generales

a. El responsable de seguridad y privacidad de la información debe generar un procedimiento para la gestión de accesos el cual debe considerar todos los sistemas, bases de datos y servicios de información de la Entidad incluyendo accesos a Internet, el uso de computación móvil y trabajo remoto, de tal manera que se documente los permisos que se otorgan a cada funcionario y contratista de la entidad, ya sea de manera genérica o específica.
b. El responsable de seguridad y privacidad de la información debe verificar el cumplimiento de las pautas establecidas relacionadas con control de accesos, registro de usuarios, administración de privilegios, administración de contraseñas, utilización de servicios de red, autenticación de usuarios y nodos, uso controlado de utilitarios del sistema, registro de eventos, protección de puertos, segmentación de redes, control de conexiones a la red y control de ruteo de red.
c. Es responsabilidad del Director de la Dirección TIC el realizar campañas de concientización a los usuarios sobre el uso apropiado de usuarios y contraseñas a partir de estrategias de uso y apropiación definidas para toda la vigencia.
d. Es responsabilidad del personal que apoya la gestión en la Dirección TIC cumplir con las siguientes funciones:
    - Implementar procedimientos para la activación y desactivación de derechos de acceso a las redes.
    - Analizar e implementar los métodos de autenticación y control de acceso definidos en los sistemas, bases de datos y servicios.
    - Implementar el control de puertos, conexión a la red y ruteo de red.
    - Implementar el registro de eventos o actividades de usuarios de acuerdo con lo definido por los propietarios de la información, así como la depuración de los mismos.
    - Definir e implementar los registros de eventos y actividades correspondientes a sistemas operativos y otras plataformas de procesamiento.

- Definir e implementar la configuración que debe efectuarse para cada servicio de red, de manera que garanticen la seguridad en su operación.
- Analizar las medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.
- Otorgar acceso a los servicios y recursos de red, únicamente de acuerdo con el pedido formal correspondiente.
- Efectuar un control de los registros de auditoria generados por los sistemas operativos y de comunicaciones.

Creación y eliminación de usuarios (Internos y Externos)

a. Los funcionarios, contratistas, outsourcing o terceros, antes de solicitar acceso a los sistemas de información deben firmar un acuerdo de confidencialidad.
b. Las cuentas de usuario de los sistemas informáticos otorgados a los funcionarios de la SDS o terceros constituyen un activo de la Entidad, que permite identificar de manera única e irrepetible a cada usuario. En ninguna circunstancia las cuentas de usuario deberán ser compartidas, transferidas, reasignadas o su contraseña revelada.
c. Las cuentas de usuario (internas/externas) creadas en los sistemas de información de la Secretaría, deben tener un identificador único y deberán solicitarse mediante un requerimiento formal, especificando su identificación, nombres y apellidos y las funciones u obligaciones contractuales que va a desempeñar, junto con la autorización del jefe inmediato del usuario. Las cuentas de usuarios externas deben ser solicitadas y autorizadas a través del Secretario, Subsecretario Corporativo o Jefe de Control Interno, según corresponda.
d. La creación de cuentas genéricas, deben contar con el aval de la Subsecretaria, Oficina, Dirección o Subdirección correspondiente, definiendo siempre una persona responsable para su gestión y administración. La persona responsable de su utilización es la encargada de notificar las novedades correspondientes de la cuenta.
e. En el momento en que un empleado o contratista se retire de la Entidad, el supervisor o jefe inmediato debe notificar su retiro (Procedimiento de desvinculación) y revisar con prontitud los archivos y documentos guardados en el computador, con el fin de reasignar las tareas y delegar específicamente la responsabilidad de estos archivos que anteriormente estaban en manos del ex-empleado.
f. El área de talento humano, los supervisores o jefes inmediatos están obligados a reportar, cualquier novedad que se presente con sus funcionarios o contratistas (vacaciones, licencias, incapacidades, permisos, etc.) mediante las herramientas dispuestas para el caso (correo, mesa de ayuda, etc), para que se gestione ante el administrador de los sistemas de información, la solicitud de activación o inactivación inmediato de accesos.
g. Cuando un funcionario o contratista se retira de la SDS o no requiere seguir utilizando los sistemas de información, el administrador de los sistemas de información debe

asegurarse que el usuario no pueda ingresar, inactivando la cuenta actual (nunca se borra), esto con el fin de guardar las bitácoras de transacciones que el usuario realizó cuando la cuenta estaba activa.

h. Las cuentas que no hayan sido utilizadas en los últimos noventa (90) días deben ser inhabilitadas dependiendo del caso.

Administración de Privilegios

a. Los propietarios de los activos de información deben aprobar o negar la asignación de privilegios a usuarios y solicitar su implementación, lo cual será supervisado por el responsable de seguridad y privacidad de la información.

Administración de Contraseñas

a. Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas, para lo cual deben cumplir los siguientes lineamientos:
   - Mantener las contraseñas en secreto.
   - Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
   - Seleccionar contraseñas de calidad, de acuerdo a las recomendaciones del personal de mesa de ayuda o la Dirección TIC:
     - Sean fáciles de recordar.
     - No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona.
     - No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.
     - Mínimo ocho (8) caracteres alfanuméricos.
   - Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
   - Cambiar las contraseñas provisionales en el primer inicio de sesión.
   - Notificar cualquier incidente de seguridad relacionado con sus contraseñas: perdida o indicio de pérdida de confidencialidad.
   - Si maneja varias contraseñas para diferentes sistemas y servicios, lo recomendable es adelantar la gestión por medio de software para gestión de contraseñas.

Acceso a la red

a. Únicamente se debe proporcionar a los funcionarios o contratistas, el acceso a los servicios para los que específicamente se les haya autorizado su uso. Se deben utilizar métodos apropiados de autenticación para el control de acceso a los usuarios remotos.

b. Se deben implementar controles adicionales para el acceso por redes inalámbricas.
c. Se debe establecer una adecuada segregación de redes, separando los entornos de red de usuarios y los servicios.

Autenticación de usuarios para conexiones externas

a. El acceso de usuarios remotos estará sujeto al cumplimiento de procedimientos de autenticación. El responsable de seguridad y privacidad de la información, en conjuntamente con el propietario del activo de información de que se trate, deben realizar una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso.

Control de acceso al sistema operativo

a. Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad.
b. Queda completamente prohibido el uso de cuentas genéricas o de administrador, para la gestión y uso dentro de los servidores y equipos de usuario final.

Control de acceso dispositivos móviles

a. Los funcionarios, contratistas y terceros se comprometen a hacer uso adecuado de los dispositivos móviles para el acceso a los servicios corporativos de movilidad, proporcionados por la entidad, tales como escritorios y aplicaciones virtuales, correo, comunicaciones unificadas, redes virtuales privadas (VPN), entre otros.

6.1.8. DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS

Responsabilidades Generales*:*

a. Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrán acceder a los ambientes de producción.
b. Los sistemas de software utilizados pueden ser adquiridos a través de terceras partes o desarrollados por personal de la Dirección de Tecnologías de la Información y las Comunicaciones o contratado para tal efecto.
c. La Dirección de TIC debe elegir, elaborar, mantener y difundir un procedimiento o lineamiento orientado al “Método de Desarrollo de Sistemas Software Seguro en la SDS”

que incluya directrices, procesos, buenas prácticas, plantillas y demás documentos que sirvan para regular los desarrollos de software en un ambiente de mitigación del riesgo y aseguramiento de la calidad teniendo como base la seguridad de la información por defecto, dentro de los sistemas de información.

d. Todo proyecto de desarrollo de software debe contar con un documento de identificación y valoración de riesgos del proyecto. La Entidad no debe emprender procesos de desarrollo – o mantenimiento – de sistemas de software que tengan asociados riesgos altos no mitigados.
e. Los sistemas de software adquiridos a través de terceras partes deben certificar el cumplimiento de estándares de calidad y seguridad de la información en el proceso de desarrollo y puesta en producción.

La persona responsable del procedimiento de desarrollo de software con el acompañamiento del responsable de seguridad y privacidad de la información debe implementar los siguientes controles:

- Guardar solo los ejecutables en el ambiente de producción.
- Llevar un registro de auditoria de las actualizaciones realizadas.
- Retener las versiones previas del sistema, como medida de contingencia.
- Definir un procedimiento que establezca los pasos a seguir para implementar las autorizaciones pertinentes, las pruebas previas a realizarse, etc.
- Denegar permisos de modificación al implementador sobre los programas fuentes bajo su custodia.

6.1.9. ASPECTOS DE LA SEGURIDAD DE LA INFORMACÍON EN LA CONTINUIDAD DE NEGOCIO

Planeación Continuidad de Negocio

La SDS diseñará y mantendrá vigente un Plan de Continuidad de Negocio que atienda los requerimientos de seguridad y privacidad de la información en la entidad según el análisis de riesgos determinado para tal fin, el cual deberá estar catalogado por niveles de acuerdo con el grado de contingencia que se deba atender, por ejemplo: Grado 1, contingencias menores que se atienden con el personal dentro de las instalaciones. Grado 2, que no se permita el ingreso al edificio, Grado 3, por desastre.

Mantenimiento del Plan de Continuidad de Negocio

La entidad realizará pruebas periódicas y mantenimiento al Plan de Continuidad de Negocio por lo menos una (1) vez en el año.

6.1.10. SEGURIDAD DE LA INFORMACION PARA LAS RELACIONES CON LOS PROVEEDORES

Consideraciones de seguridad en los acuerdos con terceras partes

a. En todos los contratos o acuerdos con terceras partes, que implique un intercambio, uso o procesamiento de información de la Entidad, se deben realizar acuerdos de confidencialidad sobre el manejo de la información, acorde con las directrices de la Subdirección de Contratación y la reglamentación definida.

b. Los acuerdos de confidencialidad de la información deben hacer parte integral de los contratos o documentos que legalicen la relación del negocio.

c. Dentro del contrato o acuerdo se deben definir claramente el tipo de información que se va a intercambiar por las partes y el uso que se le debe dar.

6.1.11. CUMPLIMIENTO

Política para el Cumplimiento y Normatividad Legal

Toda solución de servicios o infraestructura tecnológica debe garantizar que su selección está de acuerdo con las condiciones contractuales, de legislación y regulación externa e interna, para el debido cumplimiento de los regímenes legales a los cuales está sometida la Entidad.

Estándares de la Política para el Cumplimiento y Normatividad Legal

Cumplimiento legal

Todos los requerimientos contractuales y legales que puedan afectar los sistemas de información deben definirse previamente y documentarse de acuerdo con la metodología empleada por la entidad. Los controles específicos, medidas de protección y responsabilidades individuales que cumplan con los requerimientos, deben así mismo definirse y documentarse. La Subdirección de Contratación y/o la Oficina Asesora Jurídica asesorarán al Comité Institucional de Gestión y Desempeño o quien haga sus veces en dichos aspectos legales específicos.

Propiedad intelectual

Se protegerá adecuadamente la propiedad intelectual de la Entidad, tanto propia como la de terceros (derechos de autor de software o documentos, derechos de diseño, marcas registradas, patentes, licencias, código fuente, entre otros). El material registrado con derechos de autor no se debe copiar sin la autorización del propietario y se debe especificar la forma de utilización del mismo, una vez se termine el vínculo contractual.

Protección de datos

Los estándares y leyes de seguridad y privacidad de la información son de obligatorio cumplimiento para los funcionarios y contratistas de la Entidad con acceso a los datos de carácter personal y a los sistemas de información. Deberán considerar, los siguientes aspectos:

- Ámbito de aplicación del procedimiento con especificación detallada de los recursos protegidos.
- Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido por la ley.
- Funciones y obligaciones del personal con acceso a las bases de datos.
- Estructura de las bases de datos de carácter personal y descripción de los sistemas de información que los tratan.
- Procedimiento de notificación, gestión y respuesta ante los incidentes.
- Procedimientos de realización de copias de respaldo y de recuperación de los datos.
- Controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el procedimiento de seguridad de la información que se implemente.
- Medidas a adoptar cuando un soporte o documento va a ser transportado, desechado o reutilizado.

El procedimiento se mantendrá actualizado en todo momento y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

Cumplimiento de la Política de seguridad

a. Cada responsable de Subsecretaría, Oficina, dirección y Subdirección debe velar por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad y privacidad de la información establecidos, dentro de su área de responsabilidad.
b. El responsable de seguridad y privacidad de la información y el director de la Dirección de Tecnologías de la Información y las Comunicaciones deben realizar revisiones periódicas de todas las áreas de la Entidad, a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad y privacidad desplegados.

Cumplimiento técnico

a. Se debe comprobar periódicamente que los activos de información cumplen con las normas de implementación de seguridad y privacidad definidos. Se deben realizar auditorías periódicas con ayuda de herramientas automatizadas y se deben generar informes técnicos que reflejen la evaluación de riesgos de seguridad y privacidad de la Información, vulnerabilidades y su grado de exposición al riesgo.

6.2. DIFUSIÓN A TERCEROS DE LA POLÍTICA DE LA SDS.

La política general de seguridad y privacidad de la Información de la SDS, se dará a conocer a todas las partes interesadas de la entidad, mediante los canales de comunicación existentes como los son: portal web www.saludcapital.gov.co, en link de “Transparencia y Acceso a la Información Pública” y por medio de un plan de Capacitación y sensibilización orientado a los diferentes perfiles (directivos, funcionarios, contratistas, etc.).

7. CONTROL DE CAMBIOS

VERSIÓN	FECHA DE APROBACIÓN	RAZÓN DE CREACIÓN O ACTUALIZACIÓN
1	27/02/2023	Creación de la Política general de seguridad y privacidad de la Información. Las Políticas de seguridad y privacidad de la Información tienen como objetivo principal establecer reglas sobre el uso de la información, los sistemas informáticos y de comunicaciones de la Secretaría Distrital de Salud (SDS), por parte de los usuarios, administradores o terceros, buscando la protección de los recursos de información de la Entidad y la Tecnología utilizada para su procesamiento, frente a las amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.