Secretaría Distrital de Planeación

Políticas de Seguridad de la Información

Responsable:

Comité Coordinador del SIG
Subsecretaría de Información y Estudios Estratégicos
Secretaría Distrital de Planeación

TABLA DE CONTENIDO

1. ANTECEDENTES 5
2. RESUMEN 7
3. INTRODUCCIÓN 8
4. ALCANCE 9
5. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN 10
5.1 Objetivos específicos de seguridad de la información 10
6. POLITICAS ESPECÍFICAS EXISTENTES EN EL SGSI 14
6.1 Política de Control de acceso 14
6.2 Política de Escritorio y Pantalla Limpios 14
6.3 Política para el Uso de Dispositivos Móviles de la SDP 15
6.4 Política de Gestión de Carpetas Públicas y Privadas 16
6.5 Política para la Gestión de Copias de Respaldo y Recuperación de la Información . 17
6.6 Política de Protección de Datos Personales. 18
7. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN 19
8. RESPONSABILIDADES 20
9. RESULTADOS CLAVE 21
10. POLÍTICAS RELACIONADAS 22
11. DOCUMENTACION DE REFERENCIA 23

DERECHOS DE AUTOR

AUDIENCIA

De uso interno en la Secretaría Distrital de Planeación.

1. ANTECEDENTES

En cumplimiento del Artículo 20 "DIRECTRICES DE SEGURIDAD DE LOS DATOS Y LA INFORMACIÓN" de la Resolución No. 305 de 2008 emitida por la Comisión Distrital de Sistemas (CDS) *"Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre",* que indica: *…"Los Jefes de las entidades, organismos y órganos de control del Distrito Capital para efectos de facilitar la Gestión de la Seguridad de la Información al interior de cada una de sus entidades y teniendo en cuenta las normas internacionales generalmente aceptadas, deben establecer un Comité de Seguridad de la Información, así como la aplicación de los dominios de control a que se refiere la norma NTC-ISO/IEC 27001 que establece los requisitos del Sistema de Gestión de Seguridad de la Información (SGSI) y las normas NTC-ISO/IEC 17799 con su equivalente NTC-ISO/IEC 27002 y demás normas concordantes*", la Secretaría Distrital de Planeación (SDP) lideró durante la vigencia 2010, el proceso para la conformación del Comité de Seguridad de la Información, logrando la adopción de la Resolución 1465 de 2010 por medio de la cual se creó el Comité de Seguridad de la Información (en adelante CSI) y se dictaron otras disposiciones; adicionalmente se construye y aprueba el primer documento de políticas de seguridad de la información de la Entidad que refleja los lineamientos en seguridad de la información dados por la Alta Dirección; a partir del cumplimiento de las funciones que debe desarrollar el CSI y el Grupo Interdisciplinario de Trabajo del CSI (en adelante GIT), se asegura la validación de las políticas de seguridad de la información, así como los procesos, procedimientos, y metodologías específicas para la protección de la información de la Entidad (disponibilidad, integridad y confidencialidad).

Para la vigencia 2013, el GIT, como parte de la validación periódica ejecutada sobre las políticas de seguridad de la información de la Entidad, en cumplimiento del Artículo 23 " *Responsables de la promulgación, difusión e implementación de las políticas de seguridad"* de la Resolución 305 de 2008 de la CDS, realizó ajustes buscando homologar y complementar las políticas actuales de la SDP, basándose en las recomendaciones de las normas internacionales: NTC-ISO/IEC 27001 que establece los requisitos del Sistema de Gestión de Seguridad de la Información y la norma NTC/ISO IEC 17799 con su equivalente NTC-ISO/IEC 27002 que instaura las mejores prácticas para la implementación del sistema de Gestión de Seguridad de la Información. El GIT igualmente se apoyó en las políticas definidas en el Artículo 22 de la citada resolución, donde se define una política de seguridad por cada dominio de control de la norma NTC-ISO/IEC 27001.

En lo corrido del año 2014, y debido a la actualización de la norma técnica colombiana ISO27001 de su versión 2006 a su versión 2013, se aprobó utilizar como referencia normativa para la implementación del SGSI en la SDP, la norma actualizada. Por lo anterior, el GIT realiza el ajuste sobre el documento de políticas de seguridad de la información bajo los nuevos lineamientos y recomendaciones de dicha norma, y bajo las recomendaciones dadas en el Anexo D "Estructura de las políticas" de la norma GTC-ISO/IEC 27003, documento que es revisado y aprobado por el CSI.

En el año 2016 mediante resolución 1361 del 26 de Septiembre de 2016 se deroga la resolución 1604 de 2014 con el propósito de garantizar un ejercicio articulado y armónico de cada uno de los subsistemas dando como resultado la fusión del Comité de Seguridad Información en el Comité Coordinador del Sistema Integrado con el objetivo de simplificar y racionalizar instancias y facilitar la toma de decisiones.

En la misma resolución, **"Artículo 13 Objeto y responsabilidades del Grupo Operativo del Sistema Integrado de Gestión"** se establecen las responsabilidades de dicho grupo las cuales incluyen los subsistemas entre los cuales se encuentra el de Seguridad y Privacidad de la Información por lo cual el Grupo Interdisciplinario de Trabajo no existe y sus responsabilidades se delegan al Grupo Operativo del Sistema Integrado de Gestión, según el presente artículo.

En el 2017 la Comisión Distrital emite la modificación a la Resolución 305 de 2008 mediante resolución 004 de 2017 en la cual en su ARTÍCULO 6°-: Modificar el artículo 16 de la Resolución CDS 305 de 2008, el cual en lo sucesivo tendrá el siguiente tenor: "Artículo 16. POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Las entidades, organismos y órganos de control del Distrito Capital deben adoptar políticas de seguridad y custodia de los datos y la información, y establecer los procedimientos para el adecuado uso y administración de los recursos informáticos de los cuales se valgan para cumplir con sus funciones administrativas, operativas y misionales. Las entidades, organismos y órganos de control del Distrito Capital deberán atender la normatividad y lineamientos que formulen las entidades nacionales sobre el particular, incluyendo los que han sido formulados y los que llegue a formular el MinTIC, así como los que emitan otras autoridades competentes del orden nacional (por ejemplo, el Ministerio de Defensa, la Dirección Nacional de Inteligencia y el DNP, que son citados por el CONPES 3854 de Seguridad Digital como autoridades en la materia) y que sean aplicables a la respectiva entidad".

De igual forma en el mismo año se actualiza la resolución interna por la cual se modifica y compila la reglamentación del Sistema Integrado de Gestión de la Secretaria Distrital de Planeación y se dictan otras disposiciones, siendo expedida el 8 de septiembre de 2017 con número 1508.

Finalmente, es importante tener en cuenta que el documento en sus 6 versiones anteriores se publicó en el módulo SIPA-SIG como E-LE-028 y por correcciones de nomenclatura queda actualmente como A-LE-429

2. RESUMEN

La Secretaría Distrital de Planeación a través de este documento establece la intención de la alta dirección con el proceso responsable de la gestión y protección de la información, a fin de garantizar la integridad, la confidencialidad y la disponibilidad en los activos de información, conforme a la legislación vigente y a los estándares que le aplican.

El cumplimiento de esta política es obligatorio para servidores contratistas y partes interesadas, sin excepción.

La información importante para la Entidad debe estar protegida, cualquiera sea su forma, ya sea que esté compartida, almacenada o que se haya comunicado.

3. INTRODUCCIÓN

La seguridad de la información es la protección de la información importante para la Entidad contra una amplia variedad de amenazas, con el fin de asegurar la continuidad de sus servicios y minimizar los riesgos a los que está expuesta. Dicha información puede encontrarse en diferentes formas: escrita, impresa (en papel), almacenada electrónicamente, transmitida por correo o por medios electrónicos o información suministrada personalmente.

Es importante tener en cuenta que las políticas de seguridad de la información reflejan la orientación y dirección de la alta gerencia en el desarrollo de controles de seguridad de la información sobre los recursos de información y procesos de la SDP. La política de seguridad de la información es el producto de una revisión periódica semestral, que refleja los cambios en los requerimientos de cumplimiento de regulaciones, los cambios significativos en los procesos de la Entidad y en las tecnologías de la información que aseguren su conveniencia, adecuación y eficacia continuas.

4. ALCANCE

Este documento sustenta la política de seguridad de la información para la SDP y se aplica a toda la Entidad, a sus recursos y a la totalidad de los procesos, con el objeto de gestionar adecuadamente la seguridad de la información, teniendo como marco la norma técnica NTC-ISO/IEC 27001 en su versión 2013. Se debe dar cumplimiento a la presente política y se debe dar a conocer a todo el personal de la entidad y hará parte de los procesos de inducción y reinducción, igualmente debe estar disponible para las partes interesadas, según sea apropiado.

5. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La Secretaría Distrital de Planeación lidera y orienta el proceso de planeación del Distrito Capital, siendo fundamental para la Entidad proteger la información que gestiona en la totalidad de su ciclo de vida y los medios que permiten dicho ciclo, garantizando así su integridad, confidencialidad y disponibilidad, teniendo como marco la norma técnica NTC-ISO/IEC 27001 en su versión 2013, asegurando su mejoramiento continuo.

Por lo tanto, todas las personas naturales y jurídicas que laboran para la Secretaría Distrital de Planeación serán responsables por el cumplimiento de las políticas, normas, procedimientos y estándares vigentes respecto a la seguridad de la información, permitiendo a la SDP identificar y minimizar los riesgos a los cuales se expone su información y establecer una cultura de seguridad que garantice el cumplimiento de los requerimientos legales y técnicos mediante la adopción de las mejores prácticas.

A continuación los objetivos específicos de la política de seguridad de la información.

5.1 Objetivos específicos de seguridad de la información[1]

Para cada uno de los objetivos citados a continuación se deben establecer los controles aplicables que permitan a la SDP proteger su información, los cuales deben ser implementados en **marco del plan estratégico 2016 – 2020 Objetivo 10 "Fortalecer la Gestión Administrativa para contribuir al cumplimiento de las metas institucionales mediante la mejora continua de los procesos y la prestación de servicios de manera integral y efectiva con un recurso humano comprometido**. De acuerdo con el marco de referencia ISO27001 versión 2013 definido para el establecimiento de los objetivos de seguridad de la información, la entidad debe[2]:

Dominio de control	Objetivo
Políticas de seguridad de la información	Brindar orientación y soporte para la seguridad de la información, por parte de la alta dirección, de acuerdo con los requisitos del servicio, con las leyes y reglamentos pertinentes.

[1] Tomados de la Norma NTC-ISO/IEC 27001versión 2013.

[2] Objetivos planteados por dominio de control, de acuerdo con resolución 305 de 2008, artículo 22 que indica: "*Dominios de Control". La norma NTC-ISO/IEC 27001 que establece los requisitos del Sistema de Gestión de Seguridad de la Información define los dominios de control como guía que permite garantizar la seguridad de la información…*".

Organización de la seguridad de la información	Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la Entidad. Garantizar la seguridad de la información institucional en el teletrabajo, en caso que la Entidad lo implemente.
Seguridad de los recursos humanos	Asegurar que los servidores y contratistas comprendan sus responsabilidades y sean idóneos en los roles para los que se consideran. Asegurar que los servidores y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan. Proteger los intereses de la Entidad como parte del proceso de cambio o terminación del empleo.
Gestión de activos	Identificar los activos organizacionales y definir las responsabilidades de protección adecuadas. Asegurar que la información reciba un nivel apropiado de protección, de acuerdo con su importancia para la Entidad. Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.
Control de acceso	Limitar el acceso a información y a instalaciones de procesamiento de información. Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios. Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación. Evitar el acceso no autorizado a sistemas y aplicaciones.
Criptografía	Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información, en caso que aplique para la Entidad.

Seguridad física y del entorno	Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la Entidad. Prevenir la pérdida, daño, robo o compromiso de activos y la interrupción de las operaciones de la Entidad.
Seguridad de las operaciones	Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información. Asegurar que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos. Proteger la información contra la pérdida de datos. Registrar eventos en contra de la seguridad de la información y generar evidencia. Asegurar la integridad de los sistemas operacionales. Prevenir el aprovechamiento de las vulnerabilidades técnicas. Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.
Seguridad de las comunicaciones	Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información de soporte. Mantener la seguridad de la información transferida dentro de la Entidad y con cualquier entidad externa.
Adquisición, desarrollo y mantenimiento de sistemas	Garantizar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas. Garantizar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información. Asegurar la protección de los datos usados para pruebas.

Relación con proveedores	Asegurar la protección de los activos de la Entidad que sean accesibles a los proveedores. Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.
Gestión de incidentes de seguridad de la información	Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.
Aspectos de seguridad de la información de la gestión de continuidad del servicio	Incluir aspectos de seguridad de la información en la gestión de la continuidad de los servicios de la Entidad. Asegurar la disponibilidad de instalaciones donde se realiza el procesamiento de información.
Cumplimiento	Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad. Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales. Dar cumplimiento a los requisitos establecidos en la norma ISO27001 versión 2013 (contexto de la organización, liderazgo, planificación, soporte, operación, evaluación del desempeño y mejora), los cuales deben ser plasmados en un plan de trabajo que permita abordarlos, y que debe ser aprobado por la alta dirección de la Entidad (CSI).

6. POLITICAS ESPECÍFICAS EXISTENTES EN EL SGSI

En el proceso de implementación del SGSI, se cuenta con una serie de políticas específicas que han sido creadas en cumplimiento de los controles establecidos por la norma ISO 27001 versión 2013 las cuales se encuentran en el Sistema Integrado de Gestión y hacen parte de la diaria operación.

Entre ellas tenemos:

6.1 Política de Control de acceso

La política de control de acceso va orientada no solo al acceso lógico a la información sino al acceso físico y se deben considerar en conjunto por lo cual en la política y los procedimientos que la acompañan se da una visión clara de cómo se deben cumplir los controles y las responsabilidades que cada uno tiene sobre dichos accesos.

Entre los aspectos más importantes que se contemplan en ella tenemos

- Gestión del acceso de usuarios.
- Requisitos de la entidad para el control de acceso.
- Control de acceso a las aplicaciones
- Control de acceso a la información.
- Responsabilidades de los usuarios.
- Control de acceso a las redes.
- Control de acceso al sistema operativo.
- Control de acceso a las aplicaciones y a la información.
- Control de acceso en Teletrabajo.
- Control de acceso a la Gestión Documental en la SDP

En la Entidad se establecen las reglas en materia de control de acceso en el documento **"A-LE-315 POLÍTICA DE CONTROL DE ACCESO"** cuyo objetivo es limitar el acceso a la información que gestiona la Entidad al personal autorizado de forma explícita y específica por parte del dueño de la información en la SDP.

6.2 Política de Escritorio y Pantalla Limpios

La política de control de escritorio y pantalla limpios, busca controlar el acceso lógico a la información cuando un equipo queda desatendido, bloqueando al momento de dejarlo y al acceso a la información física que reposa en los escritorios de los servidores de la entidad.

Entre los aspectos más importantes que se contemplan en ella tenemos

- Debe ser cumplida por servidores, contratistas y pasantes de la SDP.
- Toda persona debe ser anunciada cuando se dirija a un puesto de trabajo
- Bloqueo de las sesiones en equipos al momento de retirarse del mismo.
- Contempla la obligatoriedad de apagar el equipo al momento de terminar la jornada
- Los equipos de reproducción de información deben estar controlados
- Áreas de reuniones libres una vez utilizadas
- Se debe velar el cumplimiento de la política “Cero Papel”
- Los equipos prestados para reuniones se dejaran libres de información.
- Incluye además las responsabilidades de los participantes en dicha política

En la Entidad se establecen la política en este sentido en el documento **“A-LE-317 POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIOS”** cuyo objetivo Reducir los riesgos de acceso no autorizado, pérdida o daño de la información que reposa en los puestos de trabajo u oficinas o que es procesada en equipos de cómputo, durante y fuera del horario laboral de la SDP.

6.3 Política para el Uso de Dispositivos Móviles de la SDP

La política de uso de dispositivos móviles de la SDP dicta las normas a seguir en este tipo de dispositivos.

Entre los aspectos más importantes que se contemplan en ella tenemos

- Evitar que los dispositivos móviles queden desatendidos cuando se utilizan en salas de juntas y fuera de la entidad.
- Debe ser cumplida por servidores, contratistas y pasantes de la SDP.
- Se debe proteger con el bloqueo de pantalla después de un determinado tiempo
- La copia de seguridad es indispensable para proteger la información.
- Deben ser protegidos utilizando software contra código malicioso.
- Solo activar acceso por Bluetooth, infrarrojo y wi-fi cuando se vayan a utilizar
- Incluye además las responsabilidades de los participantes en dicha política
- Instalar/habilitar funciones antirrobo
- Realizar actualizaciones del software de manera permanente.
- Cierre de todas las sesiones al terminar de usarlas

En la Entidad se establece la política en este sentido en el documento **“A-LE-321 POLÍTICA PARA EL USO DE DISPOSITIVOS MOVILES DE LA SDP**” cuyo objetivo Establecer las consideraciones básicas para gestionar los riesgos introducidos por el uso de dispositivos móviles que proporcionan servicios móviles y conectividad constante a los servidores públicos de la SDP que acceden a información de la Entidad.

6.4 Política de Gestión de Carpetas Públicas y Privadas

En la SDP se cuenta con las denominadas carpetas públicas y privadas, las cuales fueron creadas para compartir información tanto internamente en la oficina (privada) como con las demás oficinas (publica).

Entre los aspectos más importantes que se contemplan en ella tenemos

- Se tendrá permisos en las carpetas de la subsecretaría a la que pertenece.
- Generar máximo hasta tres niveles de subcarpetas dentro de la subcarpeta de su área.
- La organización y administración de las carpetas es responsabilidad de cada área.
- Se cuenta máximo con en la privada 12 Gigas por área
- La información almacenada en la pública es de carácter temporal
- La información de la privada es respaldada por la Dirección de Sistemas
- Las carpetas públicas cuentan con 100 Gigas en total, por lo cual es responsabilidad de cada usuario depurarla permanentemente.
- El borrado de la información de la pública se realiza cada 15 días
- En caso de requerirse Se dispondrán carpetas solicitadas por los Jefes del área para trabajar temas específicos.
- La solicitud para creación de una carpeta específica deberá ser tramitada por un Jefe de área por medio del A-FO-010 “Solicitud Gestión Cuentas de Usuario” a través de la Mesa de Ayuda
- Cada equipo de trabajo es responsable de la información almacenada en la carpeta específica asignada
- No se deben utilizar caracteres como tilde y ñe
- Para separar los nombres se permiten: “_” barra al piso (underscore) o “-“guion (hyphen), sólo si se requiere para dar mayor claridad.
- No use espacios en blanco para separar las palabras.
- Evite nombrar las carpetas con los nombres de los usuarios, hágalo por temas.
- El nombre de los archivos y carpetas será máximo 20 caracteres.
- Si un archivo es periódico o versionado, use formato de fecha (aaaammdd) en parte del nombre, con el fin de facilitar su búsqueda por fecha.
- Evite el uso de artículos (el, las, los, de) en el nombre del archivo.

En la Entidad se establece la política en este sentido en el documento “E-LE-027 POLÍTICA DE GESTION DE CARPETAS PUBLICAS Y PRIVADAS” cuyo objetivo principal es Generar la cultura

institucional que lleve a los servidores y servidoras públicos (usuarios) a utilizar los espacios de almacenamiento de una manera adecuada y siempre en el contexto de la gestión institucional.

6.5 Política para la Gestión de Copias de Respaldo y Recuperación de la Información

La política fue definida dado que la información que reside en los diferentes ambientes tecnológicos no está exenta de fallas o errores que puedan afectarla,

Entre los aspectos más importantes que se contemplan en la política tenemos:

- La información institucional deberá estar alojada en la infraestructura tecnológica de la entidad.
- En equipos de cómputo de servidores y/o contratistas sólo se almacenará información institucional que sea de apoyo para el procesamiento o generación de resultados.
- Para modificar o adicionar el cronograma de copias de respaldo el responsable de la información definirá el nivel adecuado de su respaldo.
- Frecuencia de los respaldos deberá estar alineada con la frecuencia con que cambia la información a respaldar.
- El periodo de retención se da acuerdo con las necesidades de cada área y basados en las tablas de retención de sus procesos.
- Se propenderá por almacenar las copias de respaldo en un sitio diferente y alejado de las sedes de la Entidad.
- Se propenderá por dar un grado apropiado de protección física y ambiental a la copia de respaldo de la información de la SDP.
- Se contará con un procedimiento para la generación de las copias a respaldar.
- Para sistemas de información, la generación de las copias de respaldo debe comprender toda la información de los sistemas, aplicaciones y datos necesarios para recuperar todo el sistema en caso de desastre.
- Para el caso de información alojada en las carpetas compartidas, la copia de respaldo se realizará de acuerdo con política de gestión de carpetas compartidas A-LE-414 publicada en SIG.
- Para el caso de las copias de respaldo de equipos de cómputo, los servidores y/o contratistas deberán disponer la información institucional a respaldar por defecto en el disco D de su equipo.
- El documento de política incluye las responsabilidades de cada uno de los roles que intervienen en el.

En la Entidad se establece la política en este sentido en el documento “A-LE-297 POLÍTICA PARA LA GESTION DE COPIAS DE RESPALDO Y RECUPERACION DE LA INFORMACION INSTITUCIONAL” cuyo objetivo es Establecer los lineamientos y directrices para la realización de las copias de respaldo de la información que está alojada en la infraestructura de la SDP, que permitan proteger la información de la entidad y restaurar de manera efectiva dicha información ante incidentes de seguridad que pueda afectar su confidencialidad, integridad y disponibilidad.

6.6 Política de Protección de Datos Personales.

En la Entidad se establece la política en este sentido en el documento “A-LE-289 POLÍTICA DE PROTECCION DE DATOS PERSONALES” cuyo objetivo es dar a conocer las políticas de protección de datos personales de la SDP.

7. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

Las reglas acerca de las acciones y decisiones para lograr los objetivos de seguridad de la información son las siguientes:

- Todo el personal debe conocer y responder por la seguridad de la información que gestiona en cuanto sea pertinente de acuerdo con sus funciones.
- Se deben tomar medidas para implementar los controles de seguridad de la información que apliquen, en los procesos de la Entidad.
- Se debe promover una cultura organizacional de mejora continua orientada a la seguridad de la información.
- Las máximas autoridades de la entidad deben comprometerse con la difusión, consolidación y cumplimiento de las políticas de seguridad de la información.
- Se debe hacer seguimiento a los riesgos de seguridad de la información y se deben tomar acciones cuando los cambios den como resultado riesgos que no sean aceptables.
- Se deben analizar y aplicar las medidas pertinentes en caso que se presenten situaciones que puedan poner a la Entidad en situación de incumplimiento frente a las políticas, procedimientos, leyes y reglamentos relacionados con la seguridad de la información.
- Se deben Proteger los recursos de información de la SDP y la tecnología utilizada para su procesamiento, frente a 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.
- Se deben mantener las políticas, procedimientos y en general todos los instrumentos internos que salvaguardan la seguridad de la información actualizados con los cambios normativos vigentes.
- El acceso no autorizado en todo o en parte o por fuera de lo acordado en los compromisos contractuales y/o laborales, a un sistema informático de propiedad de la SDP, protegido o no con una medida de seguridad, o mantenerse dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, así como la interceptación previa de datos informáticos en su origen, destino o en el interior, sin orden judicial, incurrirá en actos definidos como atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, definidos en la Ley 1273 de 2009.
- Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en registros, archivos, bases de datos o medios semejantes de propiedad y uso de la SDP, incurrirá en actos definidos como atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, definidos en la Ley 1273 de 2009.”

8. RESPONSABILIDADES

Las responsabilidades generales de las acciones para cumplir con los requisitos de la política y controles de seguridad de la información requeridos por la Entidad son:

- Las establecidas mediante resolución vigente para:
  - Los Líderes del Sistema Integrado de Gestión.
  - El Comité Coordinador del Sistema Integrado de Gestión.
  - El Grupo Operativo del Sistema Integrado de Gestión.
  - Los líderes y responsables del proceso.
- Cada Subsecretario, Director y Jefe de Oficina es responsable de velar por la protección de la información que se gestiona en su área de acuerdo con las políticas y normas de seguridad de la información de la SDP.
- Cada líder de proceso debe garantizar que se incluyan los lineamientos dados en las políticas y normas de seguridad de la información en sus procesos.
- Todo el personal (Servidor público, pasante y contratista) de la entidad es responsable por el manejo de la información que tenga a su cargo en cumplimiento de sus funciones.

Estos roles y otros aplicables al SGSI se encuentran detallados en el documento *"Roles y responsabilidades de seguridad de la información A-LE-009"*, publicado en el SIG.

9. RESULTADOS CLAVE

Los resultados a ser logrados por la SDP al dar cumplimiento a esta política son:

- La prestación de servicios al cliente externo e interno por parte de la Entidad estará soportada en la aplicación de controles de seguridad de la información que permitan mantener su disponibilidad, integridad y confidencialidad.
- Se generará una cultura de seguridad de la información que permita el sostenimiento del sistema de Gestión de Seguridad de la Información de la SDP.
- Se gestionarán los riesgos de seguridad de la información de acuerdo con los niveles aceptables acordados para la SDP.

10. POLÍTICAS RELACIONADAS

Las siguientes políticas brindan principios y orientación sobre aspectos de seguridad de la información:

- Política de gestión de carpetas públicas y privadas (A-LE-414)
- Política para la gestión de copias de respaldo y recuperación de la información institucional (A-LE-297)
- Política de protección de datos personales (A-LE-289)
- Política de Control de Acceso (A-LE-315)
- Política de Escritorio y Pantalla Limpios (A-LE-317)
- Política para el uso de dispositivos móviles de la SDP (A-LE-321)

En la medida que se formulen otras políticas al interior de la Entidad, deben incluirse en ellas aspectos relacionados con seguridad de la información, que se citen en este documento ya sea en esta versión o en actualizaciones posteriores".

11. DOCUMENTACION DE REFERENCIA

Para la comprensión del presente documento se toman como referencia los siguientes documentos o normas externas:

- NTC-ISO/IEC 27001:2013
- NTC-ISO/IEC 27002:2013
- NTC-ISO/IEC 27003:2005
- Modelo de Privacidad y Seguridad de la Información MSPI de MINT