POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

INTRODUCCIÓN

De conformidad con lo establecido en el decreto único reglamentario 1078 de 2015, con el decreto 1008 de 2018 de la política de Gobierno Digital, emitidos por el Ministerio de las TIC, con el decreto 1581 de 2012 de la ley de protección de datos personales, con el documento CONPES 3854 de 2016 en donde se establece la política nacional de seguridad nacional y con las políticas institucionales establecidas bajo el marco del decreto 1449 de 2017 cuyo objeto es el Modelo Integrado de Planeación y Gestión, se establecen el criterio de cumplimiento de alto nivel correspondientes a la gestión de la seguridad de la información. Dicho criterio o regla de cumplimiento deben ser acatada y cumplida por todos aquellos que gestionen activos de información de la entidad. Al criterio o regla en cuestión se le entenderá de aquí en adelante como la "**Política General de Seguridad de la Información**".

OBJETIVO

Establecer los lineamientos generales con el propósito de preservar los niveles de confidencialidad, integridad y disponibilidad de los activos de información, definiendo y asignando las responsabilidades a los funcionarios, contratistas y terceros de la <NOMBRE DE LA ENTIDAD DISTRITAL> (<SIGLA DE LA ENTIDAD>), conforme a los controles de seguridad y privacidad determinados en la entidad.

ALCANCE

La política general de seguridad de la información aplica a todos los funcionarios, contratistas y terceros <de NOMBRE DE LA ENTIDAD DISTRITAL>. De igual manera la presente política aplica a todos los procesos de la entidad bajo el marco de gestión establecido en el Modelo Integrado de Planeación y Gestión -MIPG- propuesto por el DAFP[1].

[1] Decreto 1499 de 2017, "Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 33 de la Ley 1753 de 2015".

Dicha política permitirá un manejo adecuado de la confidencialidad, integridad y disponibilidad[2] de sus activos de información, mediante una gestión continua del riesgo, la adopción de buenas prácticas en el uso de estos y la mejora de las competencias de los funcionarios de la entidad.

DETALLE

< NOMBRE DE LA ENTIDAD DISTRITAL> logrará la protección y manejo adecuado de la información de los ciudadanos del Distrito Capital, que se encuentre bajo su responsabilidad y custodia, de igual manera con la información generada en el desarrollo de su misionalidad -*que soportan los procesos de la Entidad y apoyan la implementación del Modelo de Seguridad y Privacidad de la Información*[3]- con un compromiso de la Alta Dirección.

Para la gestión estratégica y operacional de la seguridad de la información, <NOMBRE DE LA ENTIDAD DISTRITAL> se alinea con las siguientes premisas:

- Disminuir el riesgo de los procesos misionales de la entidad.
- Atender los principios de seguridad de la información[4].
- Atender los principios de la función administrativa.
- Fortalecer la confianza de los funcionarios y terceros (proveedores y contratistas).
- Apoyar las iniciativas y proyectos de innovación con tecnología.
- Implementar el SGSI.
- Proteger y salvaguardar los activos de información.
- Fortalecer la cultura de seguridad de la información en los funcionarios y terceros (proveedores, contratistas y practicantes) <del/ de la> < NOMBRE DE LA ENTIDAD DISTRITAL>
- Garantizar la continuidad de la seguridad de la información crítica del negocio frente a incidentes.

---

[2] Disponibilidad: propiedad de ser accesible y utilizable cuando se requiera por quien esté autorizado. Confidencialidad: propiedad de que la información no esté disponible o divulgada a personas, entidad o procesos no autorizados. Integridad: propiedad de exactitud y completitud. Tomado de la ISO/IEC 27000.2018.

[3] Modelo de Seguridad y Privacidad de la Información: modelo de referencia propuesto por el Ministerio de las TIC para que pueda ser adoptado por cualquier organización pública o privada con el fin de salvaguardar y proteger los activos de información que estén bajo su gestión y custodia. http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

[4] Los principios de la seguridad de la información de acuerdo con lo establecido en el Modelo de Seguridad y Privacidad de la Información se encuentran enunciados en la sección “Principios de seguridad” y se hace referencia estos en la guía #2 “Elaboración de la política general de seguridad y privacidad de la información”.

PRINCIPIOS DE SEGURINFO

Definiendo un punto de partida para la gestión de seguridad de la información, se establecen once (11) principios que soportan la seguridad de la información, los cuales son:

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
- <Nombre de la Entidad Distrital> protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
- <Nombre de la Entidad Distrital> protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- <Nombre de la Entidad Distrital> protegerá su información de las amenazas originadas por parte del personal.
- <Nombre de la Entidad Distrital> protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- <Nombre de la Entidad Distrital> controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- <Nombre de la Entidad Distrital> implementará control de acceso a la información, sistemas y recursos de red.
- <Nombre de la Entidad Distrital> velará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- <Nombre de la Entidad Distrital> velará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- <Nombre de la Entidad Distrital> velará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- <Nombre de la Entidad Distrital> velará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

OBLIGACIONES ESPECIFICAS

Los funcionarios, contratistas, proveedores, usuarios o terceras partes son responsables por el manejo adecuado y aseguramiento de la información utilizada en el desarrollo de sus actividades y obligaciones contractuales.

Las partes interesadas mencionadas, deberán cumplir con los lineamientos, requisitos y buenas prácticas de seguridad de la información que adopte la entidad y que harán parte de la documentación de la gestión de seguridad los cuales se encuentran en <el manual de seguridad de la información | la intranet institucional | otro>, previniendo, detectando y reportando cualquier incidente[5] relacionado con la seguridad de la información.

Cualquier contravención u omisión de las políticas aquí descritas se sancionarán conforme a lo establecido en el **CÓDIGO DISCIPLINARIO UNICO (LEY 734 DE 2002**), así como lo definido en el Proceso Control Disciplinario establecido por <la/el> <NOBRE DE LA ENTIDAD> y se desarrollará bajo el debido proceso administrativo que haya a lugar.

[5] Incidente de seguridad de la información: uno o varios eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones del negocio (procesos misionales) y amenazar la seguridad de la información. [Tomado de ISO/IEC 27000.2018].