Plan de seguridad y privacidad de la información

2024

Secretaría Distrital de Ambiente

Dirección de planeación y sistemas de información ambiental - DPSIA

Secretaría Distrital de Ambiente
Bogotá, Colombia
2024

Secretaría Distrital de Ambiente
Av. Caracas N0 54-38
PBX: 3778899
www.ambientebogota.gov.co
Bogotá D.C. Colombia

Contenido

Tablas

Introducción

La Secretaría Distrital de Ambiente - SDA adoptó el Sistema de Gestión de Seguridad de la Información-SGSI siguiendo las recomendaciones dispuestas en el Modelo de Seguridad y Privacidad de la Información - MSPI del Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, como una herramienta para garantizar la confidencialidad, integridad y disponibilidad de la información, administrando los riesgos, cumpliendo con la legislación vigente y, generando una cultura de seguridad de la información en los servidores públicos y demás partes interesadas

Consciente de las necesidades derivadas de las necesidades del SGSI, y teniendo en cuenta que, el activo más importante y más difícil de recuperar en caso de pérdida, es sin lugar a duda la información, siendo una premisa para la Secretaría Distrital de Ambiente, por tal razón, la Entidad adelanta actividades para tratar efectivamente la confidencialidad, integridad y disponibilidad de sus activos de información, y el proceso operativo de la SDA, estas actividades se plasman en diferentes planes, como lo es el *Plan de seguridad y privacidad de la información 2024* que se presenta en este documento. Así mismo, es importante mencionar que, actualmente se implementan cambios de manera acelerada hacia una sociedad digital, con el avance de la tecnología de la información, los ataques que atentan contra los pilares de la seguridad también se han convertido en un riesgo importante para las personas, las empresas y los gobiernos. Es un hecho que los incidentes van en constante aumento amenazando la seguridad informática, la seguridad de la información y la ciberseguridad de todas las organizaciones públicas y privadas a nivel mundial.

En un entorno cada vez más interconectado, la información está expuesta a una gran cantidad y diferentes tipos de riesgos. Las amenazas como la suplantación, robo de información, los códigos maliciosos y los ataques de denegación de servicio (DOS y DDOS) se han vuelto cada vez más comunes.

La implementación, el mantenimiento y la actualización de la seguridad de la información es un gran desafío que debe enfrentar cada entidad. Con la ayuda de la seguridad de la información, desde un punto de vista estratégico y táctico la SDA puede proteger la información y la tecnología previniendo, detectando y respondiendo ante posibles amenazas internas y externas. La estrategia de seguridad de la información es responsabilidad tanto de TI (táctico) como de la alta dirección (estratégico).

Es muy importante para el apoyo de la estrategia que todo el personal de la Entidad (operativo) se concientice de los actuales problemas de seguridad de la información y adopten las medidas, las capacidades e iniciativas adecuadas para mejorar los procesos y procedimientos, con el fin de mitigar posibles riesgos de seguridad de la información en la SDA .

1. Objetivos

1.1. Objetivo General

Definir y desarrollar las diferentes actividades para la vigencia 2024, relacionadas con el Subsistema de Gestión de Seguridad de la Información (SGSI), para maximizar la seguridad y privacidad de la información, en articulación con el PETI, dando cumplimiento a la normatividad vigente y al Modelo de Seguridad y Privacidad de la Información (MSPI).

1.2. Objetivos Específico

- Gestionar las actividades de seguridad y privacidad de la información, Seguridad Digital, de acuerdo con los contextos establecidos en la Entidad en el Plan Estratégico de Tecnologías de la Información – PETI – 2020-2024.
- Contribuir con el fortalecimiento y apropiación de conocimiento sobre el Sistema de Gestión de Seguridad de la Información.
- Adelantar la gestión adecuada y efectiva de Seguridad de la información de la Entidad, con la oportunidad requerida.
- Propiciar las acciones conducentes al cierre de brechas establecidas en la Entidad en el Plan Estratégico de Tecnologías de la Información – PETI – 2020-2024
- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana y que tienen relación con Seguridad de la Información.
- Fortalecer la cultura de la entidad para proteger la información de los colaboradores y la Secretaría Distrital de Ambiente..

2. Marco normativo

Con base en el Plan Estratégico de Tecnologías de la Información – PETI – 2020-2024, el Manual del Subsistema de Gestión de Seguridad de la Información de la entidad, las políticas del Sistema de Gestión de Seguridad de la Información de la Secretaría Distrital de Ambiente, se incluye una gran variedad de disposiciones de rango constitucional, legal y reglamentario, que rigen diversas actividades en cuanto al entorno de la seguridad digital y que resultan vitales en el desarrollo de las actividades asociadas a la seguridad de la información.

2.1. Normatividad Colombiana

A continuación, se presentan las principales disposiciones que conforman el marco normativo a nivel nacional como referente para tal efecto:

Tabla 1. Normatividad Vigente

NORMA	CONTENIDO
Constitución Política de Colombia	Artículos 13, 15, 20, 21, 22, 44, entre otros. Se destacan a manera de ejemplo el Art. 15, el cual dispone: *"Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución (…)"*; así como el Art. 20, en el cual se establece que: *"Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios de comunicación masiva. Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura."*.
Ley 527 de 1999 (Comercio electrónico)	Se define y se reglamenta el acceso y uso de los mensajes de datos, el comercio electrónico y de las firmas digitales, y se establece certificación y se dictan otras disposiciones. Se tratan conceptos como: mensaje de datos(artículos 2º y 5º), el principio de equivalencia funcional (artículos 6, 8, 7, 28, 12 y 13), la autenticación electrónica (artículo 17), la firma electrónica simple (artículo 7), la firma digital (artículo 28), y la firma electrónica certificada (artículo 30, modificado por el artículo 161 del decreto ley 019 de 2012).
Ley 594 de 2000 (Ley general de archivos)	Habilita el uso de nuevas tecnologías de manera general, lo cual viabiliza el uso de firmas electrónicas simples, certificadas y firmas digitales.
Ley 599 de 2000 (Código penal)	En particular las materias atinentes a: i) violación a los derechos patrimoniales de autor y derechos conexos (modificación introducida por la Ley 1032 de 2006); ii) protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las TIC (modificación introducida por la Ley 1273 de 2009)
Ley 679 de 2001 (Pornografía y	Esta ley contempla en el artículo 6 un sistema de autorregulación, en virtud del cual el Gobierno Nacional, por intermedio del Ministerio de Comunicaciones hoy Ministerio de Tecnologías de la Información y las Comunicaciones, promoverá e

NORMA	CONTENIDO
explotación sexual con menores)	incentivará la adopción de sistemas de autorregulación y códigos de conducta eficaces en el manejo y el aprovechamiento de redes globales de información. Estos códigos se elaborarán con la participación de organismos representativos de los proveedores y usuarios de servicios de redes globales de información.
Ley 962 de 2005 (Racionalización de trámites y procedimientos)	Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos. Se destaca el numeral 4 del Art. 1º, el cual dispone que: *"(…) serán de obligatoria observancia los siguientes principios como rectores de la política de racionalización, estandarización y automatización de trámites, a fin de evitar exigencias injustificadas a los administrados:* *(…) 4. Fortalecimiento tecnológico. Con el fin de articular la actuación de la Administración Pública y de disminuir los tiempos y costos de realización de los trámites por parte de los administrados, se incentiva el uso de medios tecnológicos integrados, para lo cual el Departamento Administrativo de la Función Pública, en coordinación con el Ministerio de Comunicaciones, orientará el apoyo técnico requerido*
Ley 1150 de 2007 (Medidas para la eficiencia y la transparencia)	Mediante esta Ley se introducen medidas para la eficiencia y la transparencia en la contratación estatal, estableciendo en su Art. 3º, el sistema electrónico para la contratación pública (SECOP).
Ley Estatutaria 1266 de 2008 (Habeas data)	Contempla las disposiciones generales en relación con el derecho de hábeas data y se 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 medio de esta Ley se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado *"de la protección de la información y de los datos"*, y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1336 de 2009 (Explotación, pornografía y el turismo sexual con niños)	Se adiciona y robustece la ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes. Esta ley establece dos medidas para contrarrestar la explotación sexual y la pornografía infantil que se relacionan tangencialmente con las TIC. En primer lugar, establece en el artículo 4 (autorregulación de café internet códigos de conducta) que todo establecimiento abierto al público que preste servicios de internet o de café internet deberá colocar en un lugar visible un reglamento de uso público adecuado de la red, y deberá indicar que la violación a este genera la suspensión del servicio al usuario.
Ley 1341 de 2009 (Sector TIC)	Mediante esta Ley se definen principios y conceptos sobre la sociedad de la información y la organización de las TIC, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones. Especialmente los artículos 4, 11 y 26.
Ley 1437 de 2011 (Uso de medios electrónicos procedimiento administrativo)	Consagra la utilización de medios electrónicos en el procedimiento administrativo y permite adelantar los trámites y procedimientos administrativos, el uso de registros electrónicos, de documentos públicos en medios electrónicos, notificaciones electrónicas, archivos electrónicos de documentos, expedientes y sedes electrónicos.

NORMA	CONTENIDO
	Lo anterior, con el fin de que los ciudadanos interactúen con validez jurídica y probatoria. Especialmente los artículos 59 al 64.
Ley 1453 de 2011 (Seguridad ciudadana)	Por medio de la cual se reforma el código penal, el código de procedimiento penal, el código de infancia y adolescencia, las reglas sobre extinción de dominio y se dictan otras disposiciones en materia de seguridad. Especialmente el Art. 53, que modifica el Art. 236 de la Ley 906 de 2004.
Ley 1564 de 2012 Código General del Proceso	Art. 103, el cual permite el uso de las TIC en todas las actuaciones de la gestión y trámites de los procesos judiciales con el fin de facilitar el acceso a la justicia.
Ley 1581 de 2012 (Habeas data)	Se dictan disposiciones generales para la protección de datos. Esta ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como recolección, almacenamiento, uso, circulación o supresión por parte de entidades de naturaleza pública y privada, sin embargo, a los datos financieros se les continúa aplicando la ley 1266 de 2008, excepto los principios.
Ley estatutaria 1621 de 2013 (Para la función de inteligencia y contrainteligencia en Colombia)	Expide normas para fortalecer el marco jurídico que permita a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir adecuadamente con su misión constitucional y legal.
Ley 1712 de 2014 (Uso de las TIC)	Regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantías del derecho y las excepciones a la publicidad de la información. Toda persona puede conocer sobre la existencia y acceder a la información pública en posesión o bajo control de los sujetos obligados. El acceso a la información solamente podrá ser restringido excepcionalmente.
Decreto 1704 de 2012 (Interceptación legal de comunicaciones)	Determina que la interceptación legal de comunicaciones es un mecanismo de seguridad pública que busca optimizar la labor de investigación de los delitos que adelantan las autoridades y organismos de inteligencia. De esta manera, se determina que los proveedores que desarrollen su actividad comercial en el territorio nacional deben implementar y garantizar en todo momento la infraestructura tecnológica necesaria que provea los puntos de conexión y de acceso a la captura del tráfico de las comunicaciones que cursen por sus redes, para que los organismos con funciones permanentes de policía judicial cumplan, previa autorización del fiscal general de la nación, con todas las labores inherentes a la interceptación de las comunicaciones requeridas.
Decreto 2758 de 2012 (Modifica la estructura del Ministerio de Defensa)	Se reestructura la organización del Ministerio de Defensa Nacional, en el sentido de asignar al despacho del viceministro la función de formular políticas y estrategias en materia de ciberseguridad y ciberdefensa. Adicionalmente, le encarga a la Dirección de Seguridad Pública y de Infraestructura, la función de implementar políticas y programas que mantengan la seguridad pública y protejan la infraestructura, así como hacerle seguimiento a la gestión relacionada con el riesgo cibernético en el sector defensa y diseñar el plan estratégico sectorial en materia de ciberseguridad y ciberdefensa.

NORMA	CONTENIDO
Decreto ley 019 de 2012 (Entidades de certificación digital)	Establece las siguientes actividades que las entidades de certificación acreditadas podrán realizar en el país, tales como: producir certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas, emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles, y publicar certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la ley 527 de 1999, entre otras. Especialmente los Art. 70 y 71.
Decreto 0032 de 2013 (Creación de la Comisión nacional digital y de información estatal)	El Ministerio de Tecnologías de la Información y las Comunicaciones en cumplimiento de los lineamientos señalados en el documento CONPES 3701, creó, a través de este decreto, la Comisión Nacional Digital y de Información Estatal cuyo objeto es la coordinación y orientación superior de la ejecución de funciones y servicios públicos relacionados con el manejo de la información pública, el uso de infraestructura tecnológica de la información para la interacción con los ciudadanos y el uso efectivo de la información en el Estado colombiano.
Ley 1712 del 2014	La Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional es la herramienta normativa que regula el ejercicio del derecho fundamental de acceso a la información pública en Colombia.
Decreto 1078 de 2015	Decreto Único Reglamentario del sector TIC. En particular las normas atinentes a la Estrategia de Gobierno en Línea.
Decreto 415 de 2016	Se adiciona el decreto único reglamentario del sector de la función pública, decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones; Arts. 2.2.35.5; 2.2.35.6
Resolución SIC No. 76434 de 2012 (Habeas data)	Resolución expedida por la SIC, por medio de la cual se imparten instrucciones relativas a la protección de datos personales, en particular acerca del cumplimiento de la ley 1266 de 2008, sobre reportes de información financiera, crediticia, comercial de servicios y la proveniente de terceros países.
Resolución 3933 de 2013 del Ministerio de Defensa Nacional	Creó el Grupo ColCERT y asignó funciones a la dependencia de La Dirección de Seguridad Pública y de Infraestructura del Ministerio de Defensa Nacional respecto a promover el desarrollo de capacidades locales o sectoriales para la gestión operativa de los incidentes de ciberseguridad y ciberdefensa en las infraestructuras críticas nacionales, el sector privado y la sociedad civil.
Resolución CRC 5050 de 2017	Por medio de esta Resolución, *"(…) se compilan las Resoluciones de Carácter General vigentes expedidas por la Comisión de Regulación de Comunicaciones*".
Resolución MINTIC No. 1519 de 2020	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
Circular externa SIC 02 del 3 de noviembre de 2015	La Superintendencia de Industria y Comercio impartió instrucciones a los responsables del tratamiento de datos personales, personas jurídicas de naturaleza privada inscritas en las cámaras de comercio y sociedades de economía mixta, para efectos de realizar la inscripción de sus bases de datos en el Registro Nacional de Bases de Datos a partir del 9 de noviembre de 2015.

Fuente: Elaboración propia, adaptada de Modelo Nacional de Gestión de Riesgos de Seguridad Digital[1]

Además de la anterior normatividad, existe un modelo que suministra el Ministerio de Tecnologías de la Información denominado el Modelo de Seguridad y Privacidad de la Información - MSPI, el cual imparte los lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información, permitiendo habilitar la implementación de la Política de Gobierno Digital. Este modelo es la referencia y guía principal para la gestión del SGSI de la Secretaría.

Respecto a lo relacionado con la gestión de riesgos, el presente plan se articula con el plan de tratamiento de riesgos, la metodología de activos de información y la política de riesgos de la secretaría, incluyendo los instrumentos diseñados para estos fines.

3. Política General de seguridad y privacidad de la SDA

La secretaría cuenta con sus políticas de seguridad y privacidad de la Información, las cuales se encuentran formalmente aprobadas y son de obligatorio cumplimiento por todos los colaboradores de la Entidad, el objetivo es establecer políticas de seguridad para preservar la confidencialidad, integridad, disponibilidad de los activos de información, la protección de datos personales, mediante la gestión de los riesgos, que permite además establecer un marco de confianza a las partes interesadas en concordancia con la plataforma estratégica de la entidad.

3.1. Objetivos de las políticas de seguridad y privacidad

- Proteger la información de la SDA y de todos los grupos de interés en el marco de su gestión, salvaguardando su confidencialidad, integridad y disponibilidad a través del establecimiento de políticas para mitigar los riesgos que vulneren los activos de información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y demás colaboradores de la SDA.
- Generar confianza en los ciudadanos, colaboradores y demás grupos de interés en las gestiones que se adelanten con la SDA.

[1] República de Colombia. Modelo Nacional de Gestión de riesgos de seguridad digital. Recuperado de www.mintic.gov.co/portal/articles-61854_documento.docx., Páginas 61 a 68. Bogotá D. C.

- Gestionar y mitigar los riesgos que se puedan presentar para proteger los activos de información de la SDA contra ataques, intrusiones, robo, accesos no autorizados y fuga de información que afecte a la imagen, los intereses y el buen nombre de la SDA.
- Propender por un nivel apropiado de concientización, conocimientos y habilidades necesarios para minimizar la ocurrencia de incidentes de seguridad de la información.
- Garantizar la continuidad del negocio frente a la ocurrencia de incidentes.
- Proteger los activos tecnológicos.

3.2. Alcance del plan de seguridad y privacidad de la información de la SDA

El Sistema de Gestión de la Seguridad de la Información (SGSI) de la Secretaría Distrital de Ambiente, cubre todos los procesos y procedimientos asociados al Sistema Integrado de Gestión, siguiendo el estándar de la norma NTC-ISO-IEC 27001 y los elementos complementarios del Modelo de Seguridad y Privacidad de la Información MSPI orientados por MINTIC, la política Digital y la guía de Riesgos generada por el DAFP.

4. Plan de implementación

El Plan de implementación del presente plan, se resume en la siguiente tabla, donde se enuncian el ámbito de gestión, hitos relevantes, meta, resultado(s) esperado(s), responsables y estimación temporal inicial que denota la periodicidad de seguimiento y control. Para tal efecto, se parte de los enunciados contenidos en el Plan Estratégico de Tecnologías de la Información 2020 – 2024 de la SDA., a fin de propiciar el cierre primario de brechas que éste determina, así como las recomendaciones de mejora dadas por la oficina de control interno.

Tabla 2. Plan de implementación

ÁMBITO	META	RESULTADO	RESPONSABLE(S)	TIEMPO EJECUCIÓN
Direccionamiento Estratégico	Realizar revisiones aleatorias sobre el cumplimiento de las políticas del SGSI y sus controles.	Alto: Porcentaje de cumplimiento en el rango de [95%-100%]	Líder de Seguridad de la Información. Profesional de Seguridad de la Información. Asesor de TI de la DPSIA	01 de enero de 2024 hasta 31 de diciembre de 2024
Adelantar las actividades asociadas con la sensibilización y apropiación del SGSI.	Adelantar actividades de socialización y sensibilización sobre la gestión de Seguridad de la Información.	Medio alto: Porcentaje de cumplimiento en el rango de [60%, 80%]	Líder de Seguridad de la Información y Profesional de Seguridad de la Información.	01 de enero de 2024 hasta 30 de junio de 2024 / 01 de julio de 2024 hasta 31 de diciembre de 2024
Operación de Servicios Tecnológicos	Realizar la gestión necesaria para contar con los ejercicios de Pen testing y análisis de vulnerabilidades necesarios.	Medio Alto: Porcentaje de cumplimiento en el rango de [70%, 95%]	Líder de Seguridad de la Información y Profesional de Seguridad de la Información.	01 de enero de 2024 hasta 31 de diciembre de 2024
Calidad y Seguridad de los Componentes de Información	Atender hallazgos, incidentes y solicitudes, relacionadas con seguridad de la Información.	Alto: Porcentaje de cumplimiento en el rango de [80%, 100%]	Líder de seguridad de la Información y Profesional de Seguridad de la Información.	01 de enero de 2024 hasta 31 de diciembre de 2024
Calidad y Seguridad de los Componentes de Información	Hacer seguimiento sobre los indicadores de seguridad de la Información	Medio alto: Porcentaje de cumplimiento en el rango de [60%, 80%]	líder de seguridad de la Información y Profesional de Seguridad de la Información.	01 de julio de 2024 hasta 31 de diciembre de 2024

ÁMBITO	META	RESULTADO	RESPONSABLE(S)	TIEMPO EJECUCIÓN
Direccionamiento Estratégico	Cumplir con las actividades del plan de mejoramiento generado por la auditoría de Control Interno.	Alto: Porcentaje de cumplimiento en el rango de [80%, 95%]	Seguimiento y evaluación por la Oficina de control Interno, y aplicación por parte del Líder de Seguridad de la Información y Profesional de Seguridad de la Información.	01 de enero de 2024 hasta 30 de junio de 2024 / 01 de julio de 2024 hasta 31 de diciembre de 2024

Fuente: elaboración propia

5. COMPROMISOS

El liderazgo de la alta dirección es esencial para el desarrollo y cumplimiento de las actividades establecidas en el plan de seguridad y privacidad de la información propuesto en este documento; de esta manera se logran los beneficios esperados, se genera el impacto positivo para la Entidad y se cumplen con los objetivos definidos. Dicho lo anterior, es necesario que la alta dirección se apropie de las políticas de seguridad de la información y exija su cumplimiento, para que todo el personal de la Entidad comprenda qué pretende en cuanto a la gestión de seguridad de la información durante la vigencia, y así lograr que las actividades definidas en este plan sean realizables y evitar que éste pueda volverse obsoleto.

Por otra parte, es importante que la Entidad cuente con la capacidad humana y operativa idónea, experimentada y suficiente en lo relacionado con gestión de seguridad de la información e informática, para llevar a buen término el cronograma propuesto para el año 2024.

LISTADO DE VERSIONES

VERSIÓN	DESCRIPCIÓN DEL CAMBIO	FECHA	AUTOR(ES)
1.0	Versión inicial del documento formulación 2022	2022/01/15	Frederick Nicolai Ferro Mojica
2.0	Actualización vigencia 2023	2023/01/15	Luis Alejandro Ruiz Alonso / Frederick Nicolai Ferro Mojica
3.0	Actualización vigencia 2024	2023/12/15	Luis Alejandro Ruiz Alonso /Francisco Daza /Frederick Ferro