Plan de seguridad y privacidad de la información 2021

Dirección de planeación y sistemas de información ambiental - DPSIA

Secretaría Distrital de Ambiente
Bogotá, Colombia
2021

Secretaría Distrital de Ambiente
Av. Caracas N^{0} 54-38
PBX: 3778899
www.ambientebogota.gov.co
Bogotá D.C. Colombia

LISTADO DE VERSIONES			
Versión	Descripción del cambio	Fecha	Autor(es)
1.0	Versión inicial del documento aprobado por Comité Institucional de Gestión y Desempeño sesión No. 1 del 29 de enero de 2021	16/01/2021	Oscar A. Fajardo Ortega

Contenido

Pág.

Lista de tablas

Pág.

Introducción

El mundo actual de los negocios, de la política, incluso de la vida cotidiana y desde luego, del qué hacer de las organizaciones y personas, que hacen parte de éstas, es cada que cada vez más digital, donde todos dependen de la información y las tecnologías conexas a ella. En una u otra medida, bien sea que se haga uso de equipos médicos, sistemas de control asistidos por computador o simplemente los teléfonos inteligentes, están soportados en tecnología informática y de comunicaciones, por lo que es posible afirmar que la seguridad de la información se convierte en la necesidad básica de la vida humana y de las organizaciones de toda índole, a nivel local y global.

Como ha sido enunciado, para las organizaciones y desde luego, para la Secretaría Distrital de Ambiente, el activo más importante es la información y para garantizar la confidencialidad e integridad de la información valiosa y crucial y el proceso operativo en una organización, la demanda de seguridad de la información aumenta día a día. En la actualidad, se implementan cambios de manera acelerada hacia una sociedad digital y, con el avance de la tecnología de la información, los ataques que atentan contra la confidencialidad, integridad y privacidad también se han convertido en un riesgo importante para las personas, las empresas y los gobiernos. Es un gran hecho que la seguridad informática, seguridad de la información y la ciberseguridad nos desafían de una manera que ninguna amenaza ha enfrentado antes.

En un entorno donde cada vez se está más interconectado, los datos están expuestos a una gran cantidad y diferentes tipos de riesgos. Las amenazas como la piratería informática, los códigos maliciosos y los ataques de denegación de servicio (DOS) 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 la entidad. Con la ayuda de la seguridad de la información, una organización puede proteger la información y la tecnología previniendo, detectando y respondiendo ante amenazas internas y externas. La estrategia de seguridad de la información es responsabilidad tanto de TI como de la alta dirección. Es muy importante para el apoyo de la estrategia que todo el personal de la organización sea consciente de estos problemas de seguridad de la información con la capacitación e iniciativa adecuadas.

1 Objetivos

Objetivo General

Desarrollar las diferentes actividades del Subsistema de Gestión de Seguridad de la Información (SGSI) que viene adelantando la entidad, para maximizar la seguridad y privación de la información y continuidad de negocio, en articulación con el PETI, dando cumplimiento a los lineamientos legales y la NTC/IEC ISO 27001:2013.

Objetivos Específicos

- Gestionar los programas y proyectos de seguridad y privacidad de la información, Seguridad Digital y Continuidad de la Operación, de acuerdo con los contextos establecidos en la Entidad en el Plan Estratégico de Tecnologías de la Información – PETI – 2020-2024.

- Contribuir al fortalecimiento y apropiación de conocimiento sobre el Sistema de Gestión de Seguridad de la información de la Entidad

- 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.

2 Marco normativo

Este acápite incorpora, con fundamento 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 subsistema de gestión de seguridad de la información de la Secretaría Distrital de Ambiente y otras fuentes, 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 del modelo de gestión de riesgos de 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: Marco normativo aplicable

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 masivos de comunicación.* *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 2° y 5°), 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.

NORMA	CONTENIDO
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 explotación sexual con menores)	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 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. 1°, 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 incentivará 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 por las entidades y organismos de la Administración Pública. (…)".*
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. 3°, 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 habeas 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.

NORMA	CONTENIDO
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 electrónicos y sedes electrónicas. 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.
Resolución CRC 5050 de 2017	Por medio de esta Resolución, *"(…) se compilan las Resoluciones de Carácter General vigentes expedidas por la Comisión de Regulación Comunicaciones*".
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 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

NORMA	CONTENIDO
	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.
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.
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.

NORMA	CONTENIDO
(Crea y organiza grupos internos de trabajo)	
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.
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.
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.
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
Decreto 1078 de 2015	Decreto Único Reglamentario del sector TIC. En particular las normas atinentes a la Estrategia de Gobierno en Línea.
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.

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

[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.

2.2 Referencias para la gestión de riesgo

Tabla 2: Marcos de referencia para la gestión del riesgo

MARCO DE REFERENCIA	DESCRIPCIÓN	CAMPO DE APLICACIÓN	FUENTE
NTC ISO/IEC 27005:2009	Norma internacional que provee directrices para la gestión de riesgo de seguridad de la información. La norma incluye un catálogo de amenazas y vulnerabilidades a manera de ejemplo, una herramienta de mucha utilidad cuando se está iniciando el proceso de implementación.	La norma ISO 27005 incluye un catálogo de amenazas y vulnerabilidades, muchas de ellas orientadas a TI, por lo que son útiles para la identificación del riesgo digital en el modelo.	https://www.iso.org/home.html
NTC ISO 31000:2011	Esta norma técnica colombiana, provee los principios, directrices genéricas, marco de trabajo y un proceso destinado a gestionar cualquier tipo de riesgo, en cualquier organización. Esta norma no es certificable.	Se toma como referencia, el proceso para la gestión del riesgo	https://www.iso.org/home.html
NTC 5722:2012	Contiene los requisitos para que las empresas implanten, mantengan y mejoren un sistema de gestión de continuidad de negocio. Es de las primeras normas alineadas con el esquema de alto nivel de ISO. Acatar tales requisitos conduce a que las empresas puedan recibir la certificación internacional.	Uno de los propósitos transmitidos desde la política de seguridad y los lineamientos CONPES se refiere a la continuidad de las operaciones corporativas y en especial de aquellas plataformas críticas de la infraestructura del país.	NTC 5722:2012

MARCO DE REFERENCIA	DESCRIPCIÓN	CAMPO DE APLICACIÓN	FUENTE
ISO IEC/27031:2011	Describe los conceptos y principios de la disponibilidad de tecnología de información y comunicación (TIC) para la continuidad del negocio y proporciona un marco de métodos y procesos para identificar y especificar todos los aspectos, tales como criterios de desempeño, diseño e implementación, y mejorar la preparación de las TIC para asegurar la continuidad del negocio.	*Se articula de forma natural. *Claramente se indica que uno de los roles de la preparación para gestionar la continuidad tecnológica es responder al entorno de riesgos que permanece en constante cambio. *Propone la reducción del riesgo asociado a las TIC, que se puede considerar dentro de la etapa de gestión de riesgos de continuidad en tales ejercicios.	Norma ISO IEC/27031:2011.
ISO IEC/27032:2012	Contempla la descripción y estandarización de los lineamientos para aplicar y mejorar el estado de ciberseguridad e involucrar diferentes aspectos técnicos. Este estándar consigna las mejores prácticas para asegurar el ciberespacio, las diferencias de los demás temas de seguridad generales y las enfoca hacia la gestión de riesgos del mismo ciberespacio.	Propone controles de ciberseguridad orientados a la mitigación de los riesgos y su mejora continua.	https://www.iso.org/home.html
ISO IEC/27014:2013	Esta norma provee los conceptos y principios para el gobierno de la seguridad de la información, a través de los cuales las organizaciones pueden evaluar, dirigir, monitorear y comunicar todas las actividades relacionadas con seguridad de la información.	Sistema de gestión de riesgo	https://www.iso.org/home.html

MARCO DE REFERENCIA	DESCRIPCIÓN	CAMPO DE APLICACIÓN	FUENTE
ISO IEC/38500:2015	Estándar que fija unos objetivos básicos para un buen gobierno de los procesos y decisiones empresariales relacionadas con los servicios de TI, estos objetivos son: 1. Asegurar que las partes interesadas puedan confiar en el gobierno corporativo de TI. 2. Informar y orientar al equipo directivo sobre el uso de las TIC. 3. Proporcionar herramientas para que la alta dirección pueda evaluar el gobierno de las TIC.	El gobierno corporativo de TI es la base para alinear objetivos y metas de TI con los objetivos estratégicos de las organizaciones; por lo tanto, el modelo de riesgos digitales deberá estar enmarcado o soportado en los diferentes procesos de gobierno corporativo de las TI. Uno de los objetivos de la implementación de la norma ISO38500 es el de gestionar los riesgos de forma eficiente.	https://www.iso.org/home.html
Magerit versión 3:2012	Metodología de análisis y gestión de riesgos de los sistemas de información. Implementa el proceso de gestión de riesgos de acuerdo con el ciclo PHVA, dentro de un marco de trabajo para que los órganos del Gobierno tomen decisiones y tengan en cuenta los riesgos derivados del uso de tecnologías de la información.	Se toma como base la gestión del riesgo de TI	https://administracionelectronica.gob.es/pae_Home#.Wd5Vo2jWzIU
Octave	Octave, por sus siglas en inglés. Es una metodología desarrollada por *Computer Emergency Response Team* (CERT), que tiene como objetivo facilitar la evaluación de riesgos en una organización. Metodología de análisis de riesgos, que los estudia con base en tres principios: confidencialidad, integridad y disponibilidad.	Se toma como base la gestión del riesgo de TI	https://www.cert.org/

MARCO DE REFERENCIA	DESCRIPCIÓN	CAMPO DE APLICACIÓN	FUENTE
NIST 800-30/-39	Esta metodología proporciona una guía para la realización de cada una de las etapas del proceso de evaluación de riesgos es decir, se preparan para la evaluación, realizan la evaluación y mantienen la evaluación; adicionalmente, orienta las evaluaciones de riesgos y otros procesos de gestión de riesgos de la organización	Se toma como base la gestión del riesgo de TI	https://www.nist.gov/
MIPG	El modelo integrado de planeación y gestión	Se toma como base guía para la administración del riesgo	http://www.??
ITIL / ISO 20000-1	Esta norma tiene como objetivo la evaluación y estandarización para la prestación de los servicios de tecnología con calidad y el uso de las mejores prácticas de gestión y operación tecnológica.	Gestión de riesgo.	https://www.itgovernance.co.uk/iso20000
Cobit/Isaca	Cobit ayuda a las empresas a crear el valor óptimo desde IT, mantiene el equilibrio entre la generación de beneficios, la optimización de los niveles de riesgo y el uso de recursos.	N/A	http://www.isaca.org/cobit/
Practice standard for project risk management/project Management Institute	Proporciona un punto de referencia para la profesión de gestión de proyectos. La mayor parte del tiempo define los proyectos de la gestión de riesgos como buenas prácticas.	Referencia para el manejo de riesgos en proyectos.	www.pmi.org

MARCO DE REFERENCIA	DESCRIPCIÓN	CAMPO DE APLICACIÓN	FUENTE
ISAE 3402	Antes conocida como SAS-70; es un conjunto de "buenas prácticas" para la evaluación de proveedores externos. La evaluación, cuyo objetivo es garantizar la calidad de las soluciones externalizadas, se formula de manera independiente y es aceptada dentro del sector.	Seguridad de la información.	www.isae3402.com
SSAE 16	Estándar de auditoría. Reconocido internacionalmente y el enfoque está en los controles internos y externos que posee una empresa que presta servicios a terceros.	Seguridad de la información.	http://www.aicpa.org/Pages/default.aspx

Fuente: Elaboración propia, Adaptado de Modelo Nacional de Gestión de Riesgos de Seguridad Digital[2]

[2] Ibídem

3 Política General de seguridad y privacidad de la SDA

Este capítulo presenta una revisión conceptual de los principales motivadores de negocio identificados para la SDA que direccionarán las estrategias de TI para la institución: los objetivos de desarrollo sostenible el plan nacional de desarrollo, el plan de desarrollo departamental, el plan de desarrollo distrital, el pacto por la transformación digital, el plan estratégico institucional, el modelo integrado de planeación y gestión (MIPG), la política de gobierno digital, la arquitectura TI y TOGAF y las tendencias tecnológicas actuales.

3.1 Objetivos de las políticas de seguridad y privacidad

3.1.1 Objetivo General

Mantener la confidencialidad, integridad, disponibilidad de los activos de información, y la protección de datos personales, mediante la gestión los riesgos, que permita establecer un marco de confianza a las partes interesadas en concordancia con la misión y visión de la entidad.

3.1.2 Objetivos Específicos

1. Proteger los activos de información, con base en los criterios de confidencialidad, integridad, disponibilidad, mediante la implementación de controles en los procesos de la entidad de manera coordinada con las partes interesadas.

2. Gestionar los riesgos asociados con la perdida de confidencialidad, integridad, disponibilidad y privacidad de la información dentro del alcance del Sistema de Gestión de Seguridad de la Información (SGSI).

3. Garantizar el tratamiento de los datos personales obtenidos en la entidad a los titulares de la información, en el ejercicio pleno de sus derechos. 4. Sensibilizar y entrenar al personal de la entidad en el Sistema de Gestión de Seguridad de la Información (SGSI).

3.2 Alcance del SGSI 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 27001:2013 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 dado por el DAFP.

4 PLAN DE IMPLEMENTACIÓN DEL MSPI

El Plan de implementación para el cumplimiento, seguimiento y control de Seguridad y Privacidad de la Información se resume en la siguiente tabla, donde se enuncian el ámbito de gestión, hitos relevantes, Meta, resultado(s) esperado, 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 luego de la auditoría al proceso de gestión tecnológica 2020.

Ámbito de Gestión	Meta	Resultado esperado	Responsable(s)	Estimación Temporal (Trimestre)			
				T 1	T2	T 3	T4
Direccionamiento Estratégico	Crear y/o actualizar las políticas en los siguientes aspectos: seguridad informática, seguridad de la Información y continuidad del negocio	Nivel Esperado de cumplimiento: Medio alto: con un porcentaje de cumplimiento en el rango (60%, 80%]	Líder de Gestión Documental, Líder de Seguridad de la Información, Líder SIG para Seguridad	X	X	X	X
Gestión de la calidad y seguridad de los Servicios Tecnológicos	Generar el plan de gestión de riesgos asegurando el cumplimiento de los requisitos dado para tal efecto, en cuanto a: Equipos y aplicaciones	Nivel Esperado de cumplimiento: Medio alto: con un porcentaje de cumplimiento en el rango (60%, 80%]	Líder de Seguridad de la Información Líder de gestión de riesgos de Seguridad de la información	X	X		
Gestión de la calidad y seguridad de los Servicios Tecnológicos	Implementar mecanismos de análisis y gestión de los riegos (vulnerabilidades y amenazas) asociados a su infraestructura tecnológica haciendo énfasis en aquellos que puedan comprometer la seguridad de la información o que puedan afectar la	Nivel Esperado de cumplimiento: Medio alto: con un porcentaje de cumplimiento en el rango (60%, 80%]	Líder de Seguridad de la Información	X		X	

Ámbito de Gestión	Meta	Resultado esperado	Responsable(s)	Estimación Temporal (Trimestre)			
				T 1	T2	T 3	T4
	prestación de un servicio de TI.						
Operación de Servicios Tecnológicos	Asegurar la existencia y gestión del Plan de pruebas de seguridad de la información (Test de intrusión y análisis de vulnerabilidades semestral).	Nivel Esperado de cumplimiento: Medio alto: con un porcentaje de cumplimiento en el rango (60%, 80%]	Líder de Seguridad de la Información		X		X
Calidad y Seguridad de los Componentes de Información	Implementar mecanismos que permitan reportar hallazgos de seguridad encontrados durante el uso de los servicios de información	Nivel Esperado de cumplimiento: Medio alto: con un porcentaje de cumplimiento en el rango (60%, 80%]	Líder de [Seguridad de] aplicaciones, líder de mesa de servicio y líder de seguridad de la Información	X	X	X	X
Calidad y Seguridad de los Componentes de Información	Definir los criterios necesarios para asegurar la trazabilidad y auditoría de seguridad en todos los componentes y sistemas de información de la SDA	Nivel Esperado de cumplimiento: Medio alto: con un porcentaje de cumplimiento en el rango (60%, 80%]	Líder de [Seguridad de] aplicaciones			X	X
Operación de Servicios Tecnológicos	Implementar mecanismos que permitan constatar el monitoreo y evaluación del modelo de continuidad y seguridad de la información, analizando tendencias, nuevos riesgos y vulnerabilidades y realización de auditorías periódicas	Nivel Esperado de cumplimiento: Medio alto: con un porcentaje de cumplimiento en el rango (60%, 80%]	Líder de seguridad de la Información			X	X

Ámbito de Gestión	Meta	Resultado esperado	Responsable(s)	Estimación Temporal (Trimestre)			
				T 1	T2	T 3	T4
Gestión de la calidad y seguridad de los Servicios Tecnológicos	Actualizar la Política y Plan de gestión de la seguridad con esquemas de respaldo y recuperación de información tanto de los sistemas / equipos de misión crítica sino también de los usuarios que por su criticidad lo amerite.	Nivel Esperado de cumplimiento: Medio alto: con un porcentaje de cumplimiento en el rango (60%, 80%]	Líder de infraestructura	X	X		
Direccionamiento Estratégico	Realizar auditorías internas para asegurar el cumplimiento de las funciones, actividades, responsabilidades y procesos establecidos dentro de las políticas del SGSI	Nivel Esperado de cumplimiento: Medio alto: con un porcentaje de cumplimiento en el rango (60%, 80%]	Oficina de control interno Líder de Seguridad de la Información		X		X

Fuente: elaboración propia

5 Premisas

El liderazgo, compromiso y la implicación de la alta dirección son esenciales para la implementación, el desarrollo del plan de seguridad y privacidad propuesto en este documento para así lograr los beneficios que espera la entidad y todas las partes interesadas.

En este contexto, se hace necesario que la alta dirección defina un marco normativo o cuando menos de referencia, para que todo el personal de la entidad comprenda qué pretende en cuanto a la gestión de seguridad de la información durante el período 2020 a 2024, para así lograr que los lineamientos dados en este plan sean realizables y evitar que éste pueda volverse obsoleto.

Además, durante el desarrollo y la operación del presente plan, la actitud y el convencimiento de la Alta Dirección es determinante para su implantación exitosa. Por tanto, sin la adecuada participación y compromiso de la alta dirección no se podrá lograr la implantación de un Sistema de Gestión de seguridad de la información efectivo. La capacidad de liderar a la entidad, las principales acciones a tomar, el apoyo incondicional que se debe brindar y la actitud de la dirección sin duda pueden definir el éxito en la misma, puesto que el personal se compromete con sus líderes tanto como éstos demuestren, con su actitud, su propio compromiso y en especial, hacia dónde se dirige la entidad.

Por otra parte, es importante que la entidad cuente con un equipo de recurso humano idóneo, experimentado y suficiente en procesos de gestión de seguridad de la información y seguridad informática para llevar a buen término el cronograma propuesto para el año 2021. Así pues, es dable tener en cuenta el concepto de segregación de funciones para lograr eficacia en la gestión que se espera, encargando a cada rol la tarea que le corresponde, siendo estos como mínimo y sin limitarse a ellos un oficial de Seguridad de la Información (Gestión integral del SGSI), Oficial de Cumplimiento (Trasparencia) y Oficial de Datos Personales (Privacidad)

Finalmente, se recomienda que durante y luego de implementar las acciones de mejora derivadas del proceso de auditoría realizado en el año 2020, se realicen auditorías internas basadas en la norma NTC- ISO 27001:2013 para validar el cumplimiento de los compromisos adquiridos y el mejoramiento continuo en la gestión del sistema de seguridad de la información, con recursos propios y debidamente certificados en estas áreas de conocimiento (ISO/IEC27001:2013 Auditor Interno e ISO/IEC27001:2013 Auditor Líder).