PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - 2023

PROCESO:

GESTIÓN TECNOLÓGICA

SECRETARIA DISTRITAL DE AMBIENTE

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA DE AMBIENTE
BOGOTÁ

INTRODUCCIÓN

El activo más importante y más difícil de recuperar en caso de perdida, es sin lugar a duda la información, y es una premisa que la Secretaría Distrital de Ambiente tiene totalmente claro, por tal razón, adelanta actividades para tratar efectivamente la confidencialidad, integridad y disponibilidad de sus activos de información, los datos y el proceso operativo en una organización, estas actividades se plasman en diferentes planes, como lo es el plan de seguridad de la Información 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 la seguridad informática, seguridad de la información y la ciberseguridad están siendo amenazadas y desafiadas cada vez más y de maneras cada vez más diferentes.

En un entorno que está más interconectado, los datos están expuestos 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) 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 organización (operativo) sea consciente de estos problemas de seguridad de la información y con la capacitación e iniciativa adecuadas puedan apoyar los procesos y procedimientos sobre los cuales la Seguridad de la información se apoya.

1. OBJETIVOS

1.1. Objetivo General

Definir y desarrollar las diferentes actividades para la vigencia 2023, relacionadas con el Subsistema de Gestión de Seguridad de la Información (SGSI), para maximizar la seguridad y privación de la información y continuidad de negocio, en articulación con el Plan Estratégico de Tecnologías de la Información (PETI) de la SDA (2021-2024) dando cumplimiento a la normatividad actual y la NTC/IEC ISO 27001.

1.2. Objetivos Específicos

1. Gestionar las actividades 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) de la SDA (2021-2024)

2. Contribuir con el fortalecimiento y apropiación de conocimiento sobre el Subsistema de Gestión de Seguridad de la Información.

3. Adelantar la gestión adecuada y efectiva de Seguridad de la información de la Entidad, con la oportunidad requerida.

4. Propiciar las acciones conducentes al cierre de brechas establecidas en la Entidad en el Plan Estratégico de Tecnologías de la Información (PETI) de la SDA (2021-2024)

5. Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana y que tienen relación con Seguridad de la Información.

2. MARCO NORMATIVO

Con base en el Plan Estratégico de Tecnologías de la Información (PETI) de la SDA (2021-2024), 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, 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.

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 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. 1º, el cual dispone que: *"(…) serán de obligatoria observancia los siguientes principios como rectores de la política de racionalización, estandarización y*

NORMA	CONTENIDO
	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*
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 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.
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. 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.

NORMA	CONTENIDO
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.
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

NORMA	CONTENIDO
	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	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 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]

[1] República de Colombia. Modelo Nacional de Gestión de riesgos de seguridad digital. Recuperado

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 secretaria, incluyendo los instrumentos diseñados para estos fines.

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 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 de Mintic (MRAE) y las tendencias tecnológicas actuales.

3.1 OBJETIVOS DE LAS POLÍTICAS DE SEGURIDAD Y PRIVACIDAD

1. 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.

2. 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.

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

4. Garantizar el tratamiento de los datos personales obtenidos en la entidad a los titulares de la información, en el ejercicio pleno de sus derechos.

5. Sensibilizar y entrenar al personal de la entidad en el Sistema de Gestión de Seguridad de la Información (SGSI).

---

de www.mintic.gov.co/portal/articles-61854_documento.docx., Páginas 61 a 68. Bogotá D. C.

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 dado por el DAFP.

4. PLAN DE IMPLEMENTACIÓN

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.

Tabla 2. Plan de implementación

ÁMBITO	META	RESULTADO	RESPONSABLE	TIEMPO EJECUCIÓN
Direccionamiento Estratégico	Gestionar la aprobación de las políticas de seguridad de la Información.	Alto: Porcentaje de cumplimiento en el rango de [95%-100%]	Líder de Seguridad de la Información, Líder SIG para Seguridad Asesor de TI de la DPSIA	Primer trimestre del año.
Gestión de la calidad y seguridad de los Servicios Tecnológicos	Adelantar la identificación y actualización de los riesgos de seguridad de la información (Articulado con lo establecido en el plan de tratamiento de riesgos de Seguridad de la Información).	Medio alto: Porcentaje de cumplimiento en el rango de [70%, 90%]	Líder de Seguridad de la Información Profesional de Seguridad de la información. Lideres de los procesos involucrados.	Anual.

ÁMBITO	META	RESULTADO	RESPONSABLE	TIEMPO EJECUCIÓN
Gestión de la calidad y seguridad de los Servicios Tecnológicos	Hacer seguimiento sobre la efectividad de los controles establecidos (mínimo de 3 meses) sobre los riesgos que de Seguridad de la Información (Articulado con lo establecido en el plan de tratamiento de riesgos 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.	Cuarto trimestre del año.
Adelantar las actividades asociadas con la sensibilización y apropiación del SGSI.	Implementar lo establecido en la Estrategia De Sensibilización En Temas De Seguridad De La Información De La Secretaría Distrital De Ambiente Vigencia 2022-2023	Medio alto: Porcentaje de cumplimiento en el rango de [60%, 80%]	Líder de Seguridad de la Información y Profesional de Seguridad de la Información.	Primer y segundo semestre del año.
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.	Anual.
Operación de Servicios Tecnológicos	Hacer seguimiento sobre el monitoreo	Alto: Porcentaje de cumplimiento en el rango de [90%, 100%]	Líder de Seguridad de la Información y Profesional de	Primer y Segundo semestre del año.

ÁMBITO	META	RESULTADO	RESPONSABLE	TIEMPO EJECUCIÓN
	efectuado por el SOC		Seguridad de la información.	
Operación de Servicios Tecnológicos	Hacer seguimiento sobre las alertas generadas por el monitoreo de la infraestructura tecnológica de la Secretaría, relacionadas con la confidencialidad, integridad y disponibilidad de la información.	Alto: Porcentaje de cumplimiento en el rango de [90%, 100%]	Líder de Seguridad de la Información y Profesional de Seguridad de la información.	Primer y Segundo semestre del año.
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.	Anual
Calidad y Seguridad de los Componentes de Información	Aplicar y alimentar 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.	Segundo semestre del año.
Gestión de la calidad y seguridad de los Servicios Tecnológicos	Revisar y actualizar la documentación del SGSI, para garantizar su oportunidad de aplicación.	Medio alto: Porcentaje de cumplimiento en el rango de [60%, 80%]	líder de seguridad de la Información y Profesional de Seguridad de la Información.	Primer semestre del año.
Direccionamiento Estratégico	Cumplir con las actividades del plan de mejoramiento generado de la	Alto: Porcentaje de cumplimiento en el rango de [80%, 95%]	Seguimiento y evaluación por la Oficina de control Interno, y aplicación por	Primer y segundo semestre del año.

ÁMBITO	META	RESULTADO	RESPONSABLE	TIEMPO EJECUCIÓN
	auditoría de Control Interno.		parte del Líder de Seguridad de la Información y Profesional de Seguridad de la Información.	

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 el período 2020 - 2024, 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 2023. Así pues, es necesario 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, sin limitarse solo al rol del oficial de Seguridad de la Información y un profesional para la gestión integral del SGSI.

Elaboró: Luis Alejandro Ruiz Alonso
Revisó: Frederick Ferro – Asesor de TI
Aprobó: Comité Institucional de Gestión y Desempeño – Sesión No. 1 del 25 de enero de 2023