PLAN DE TRATAMIENTO DE RIESGOS 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

La evolución continua de la tecnología, han hecho que personas y organizaciones usen éstas para incrementar su aprendizaje, productividad y en general, competitividad en los negocios. Sin embargo, casi que en igual o aún, mayor proporción, se ha incrementado el uso de la tecnología con fines delictivos orientados a afectar a las personas, organizaciones, otras infraestructuras y naturalmente, sistemas de información y tecnologías de comunicación hasta llegar a afectar la economía de toda una nación. Así mismo, la dependencia de las tecnologías de información, hace necesario que se establezcan controles para eliminar o mitigar situaciones que pueden poner en riesgo la operación, los activos de información, reputación o hasta temas financieros, entre otros; por tal razón la Secretaría Distrital de Ambiente (SDA), define el presente plan de tratamiento de riesgos, el cual se encuentra articulado con la política de riesgos de la entidad y busca contar con un Planeamiento de actividades que ayuden a mantener y mejorar la gestión de riesgos relacionados con seguridad de la información.

En Colombia, durante los últimos años se ha puesto a la vanguardia la lucha contra las amenazas en el ámbito digital con estrategias tales como: el CONPES 3854 de 2016; Modelo de Seguridad y Privacidad de MINTIC y lo consagrado en el decreto 1008 de 14 de junio 2018; adoptando, además las buenas prácticas y los lineamientos de los estándares ISO 27001, ISO 31000 y la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5, emitida por el Departamento Administrativo de la Función Pública (DAFP). De la misma forma, el apoyo de diferentes organizaciones para la prevención y gestión de incidentes (MinTIC, Grupo de Respuestas a Emergencias Cibernéticas de Colombia ColCERT, Equipo de respuesta a incidentes de seguridad informática CSIRT, - Centro Cibernético Policial de la Policía Nacional), los mecanismos de investigación (fiscalía general de la Nación, Centro Cibernético Policial) y de judicialización (rama judicial).

Para la Secretaría Distrital de Ambiente, es importante acoger la normatividad vigente, donde se han venido adoptando las medidas pertinentes, aplicables y necesarias para desarrollar e implementar durante la vigencia respectiva, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información en la entidad, con el fin de identificar las posibles acciones que se deben tomar para mitigar los riesgos existentes y maximizar las medidas de seguridad encaminadas a mantener la confidencialidad, integridad y disponibilidad de la información a lo largo de la vigencia del 2023.

1. OBJETIVOS

1.1. Objetivo General

Establecer las acciones para tratar de manera integral los riesgos relacionados con la seguridad y privacidad de la información a los que la Secretaría Distrital de Ambiente pueda estar expuesta; protegiendo y preservando la integridad, confidencialidad y disponibilidad de la información, con el fin de evitar materializaciones de situaciones que pueden afectar el cumplimiento de su Misión y el logro de su Visión Estratégica.

1.2. Objetivos Específicos

- Gestionar de manera integral los riesgos de Seguridad y Privacidad de la Información para alcanzar los objetivos, la misión y la visión institucional.
- Contribuir al fortalecimiento y apropiación de conocimiento sobre la gestión de riesgos de seguridad y privacidad de la información
- Propiciar las acciones conducentes al cierre de brechas identificadas.
- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana.

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 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.

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*

NORMA	CONTENIDO
	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 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).

NORMA	CONTENIDO
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.
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	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.

NORMA	CONTENIDO
en Colombia)	
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 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.

NORMA	CONTENIDO
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]

2.1. Referencias para la gestión de riesgos

Como parte fundamental de la implementación del plan se debe tener en cuenta la gestión de riesgos de seguridad de la información y en tal sentido se relacionan los siguientes marcos de referencia para tener en cuenta.

[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.

Tabla 2. Marco de referencia para los riesgos de seguridad de la información

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 31000:2018	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.	https://ecollection.icontec.org/colecao.aspx
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.	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.	https://www.iso.org/home.html
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. Esta estándar consigna las mejores prácticas para asegurar el ciberespacio, las	Propone controles de ciberseguridad orientados a la mitigación de los riesgos y su mejora continua.	https://www.iso.org/home.html

MARCO DE REFERENCIA	DESCRIPCIÓN	CAMPO DE APLICACIÓN	FUENTE
	diferencias de los demás temas de seguridad generales y las enfoca hacia la gestión de riesgos de este ciberespacio.		
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
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/
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	https://www.funcionpublica.gov.co/web/mipg

MARCO DE REFERENCIA	DESCRIPCIÓN	CAMPO DE APLICACIÓN	FUENTE
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.	La optimización de los niveles de riesgo y el uso de recursos.	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

Fuente: Elaboración propia, Adaptado.[2]

3. POLÍTICA DE TRATAMIENTO Y ADMINISTRACIÓN DEL RIESGO DE LA SDA

La Secretaría Distrital de Ambiente se compromete a mantener una cultura de la gestión del riesgo asociada a la responsabilidad de diseñar, adoptar y promover las políticas, planes, programas y proyectos TIC necesarios para regular los riesgos de los procesos y previniendo la corrupción, mediante mecanismos, sistemas y controles enfocados a la detección de hechos asociados a este fenómeno y fortaleciendo las medidas de control y eficiencia a lo largo del ciclo de vida de un proyecto para optimizar de manera continua y oportuna la respuesta y los controles necesarios aplicables a los riesgos, además de los de seguridad y privacidad de la Información y Seguridad Digital.

La política permite establecer como tratar y manejar los riesgos basados en valoración, tomar decisiones adecuadas y fijar los lineamientos para administración de estos; a su vez, transmiten la posición de la dirección y establecen las guías de acción necesarias a todos los colaboradores de la entidad, así:

- **Evitar:** es eliminar la probabilidad de ocurrencia o disminuir totalmente el impacto, lo que requiere la eliminación de la actividad o fuente de riesgo, eliminar la exposición y su expresión máxima es dejar una actividad.
- **Prevenir:** corresponde a la Dirección de Planeación y Sistemas de Información Ambiental, esto es, planear estrategias conducentes a que el evento no ocurra o que disminuya su probabilidad, mediante acciones como: inspecciones,

[2] Modelo Nacional de Gestión de Riesgos de Seguridad Digital

mantenimiento preventivo, políticas de seguridad, revisiones periódicas a los procesos, entre otras.

- **Reducir o mitigar**: corresponde a la protección en el momento en que se materializa el evento de riesgo. Se encuentra en esta categoría los planes de emergencia, planes de continencia, equipos de protección o respaldo personal, ambiental, tecnológico, de infraestructura, copias de respaldo, sitios y protocolos para operación alterna, entre otros.
- **Transferir**: es involucrar a un tercero para que responda en todo o en parte por el riesgo que genera una actividad. Dentro de los mecanismos de transferencia se encuentran los siguientes: contratos de seguro, transferencia explicita por medio de cláusulas contractuales, derivados financieros.

4. ACTIVIDADES PARA LA GESTIÓN DE RIESGOS

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información incluye la definición de las actividades a desarrollar para mitigar los riesgos sobre los activos, estas actividades se estructuraron siguiendo las recomendaciones de la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5, emitida por el Departamento Administrativo de la Función Pública (DAFP). A continuación, se presenta una tabla que contiene el plan de implementación:

Tabla 3. Plan de implementación

ACTIVIDAD	RESPONSABLE	RESULTADO	TIEMPO EJECUCIÓN
Revisión y Actualización de las políticas y lineamientos de gestión de riesgos de seguridad de la información.	Equipo de Seguridad de la Información.	Políticas, Lineamientos y procedimientos actualizados (si aplica).	Primer trimestre.
Actualización e Identificación y priorización de los activos de información	Equipo de Seguridad de la Información.	Activos de información identificados y Priorizados en todos los procesos	Primer trimestre.
Verificar el contexto de los diferentes procesos.	Equipo de Seguridad de la Información Y todos los Procesos.	Contexto verificado y actualizado (si aplica)	Segundo Trimestre
Identificar los riesgos	Equipo de Seguridad de la Información Y todos los Procesos.	Matriz de Riesgo con los riesgos identificados	Primer Semestre
Analizar los riesgos, identificar y valorar controles	Equipo de Seguridad de la Información Y todos los Procesos.	Matriz de Riesgo con los riesgos valorados y sus controles identificado y Riesgo residual	Segundo Semestre

ACTIVIDAD	RESPONSABLE	RESULTADO	TIEMPO EJECUCIÓN
Establecer las actividades de Tratamiento de los riesgos.	Equipo de Seguridad de la Información Y todos los Procesos.	Plan de tratamiento de riesgos identificado.	Segundo Semestre
Comunicar y consultar a los procesos	Equipo de Seguridad de la Información.	Comunicación a los procesos.	Tercer Trimestre
Iniciar los monitoreos	Equipo de Seguridad de la Información.	Comunicación a los procesos sobre el monitoreo de riesgos.	Primer y segundo semestre.

Fuente: elaboración propia[3]

Cabe mencionar que la evaluación y monitoreo de controles establecidos en la vigencia 2023, está sujeta a la aprobación de estos por parte de los lideres de cada proceso asociado, y esta actividad se realizará 3 meses después de su establecimiento, o si la periodicidad establecida para su ejecución es menor, se podrá adelantar en un periodo menor.

5. COMPROMISOS

El liderazgo y compromiso de la alta dirección y de los lideres de cada proceso asociado, son esenciales para el desarrollo del plan de tratamiento de riesgos de seguridad de la información propuesto en este documento para lograr los objetivos definidos. Dicho lo anterior, es necesario que la alta dirección se apropie de las políticas de gestión de riesgos y exija su cumplimiento, para que todo el personal de la entidad se involucre y gestione de forma efectiva los riesgos identificados, evitando situaciones que pueden afectar la información de la secretaria.

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.

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

[3] Adaptación de la Guía para la administración del riesgo y el diseño de controles en entidades públicas. Pág. 57. Año 2020. DAFP