Control de cambios

Versión	Fecha	Descripción de la modificación
01	13 de febrero de 2020	Se aprueba el Plan de tratamiento de riesgos de seguridad y privacidad de la información de la Secretaría Distrital de Gobierno.
02	16 de febrero del 2021	Se ajusta las metas para la vigencia 2021
03	31 de enero de 2022	Se realiza la actualización del plan de tratamiento de riesgos para la vigencia 2022
04	30 de noviembre 2022	Se realiza la actualización del plan de tratamiento de riesgos de seguridad de la información para la vigencia 2023
05	30 de enero de 2024	Se realiza la actualización del plan de tratamiento de riesgos de seguridad de la información para la vigencia 2024
06	28 de enero de 2025	Se realiza la actualización del plan de tratamiento de riesgos de seguridad de la información para la vigencia 2025
07	30 de enero de 2026	Se realiza la actualización del plan de tratamiento de riesgos de seguridad de la información para la vigencia 2026

Método de Elaboración	Revisa	Aprueba
El documento se actualiza de acuerdo con las indicaciones de la Oficina Asesora de Planeación y los profesionales de la Dirección de Tecnologías e Información: Carlos Javier Díaz Rodríguez, Leonardo Sisrra Rodríguez y la auxiliar administrativa Doris Páez Romero.	**Mario Alexander Ortiz Salgado** Proceso Gerencia de TIC Director de Tecnologías e Información **Olga Milena Arias Aguirre** Promotora de Mejora **Leidy Johana Avila Arias** Revisión Metodológica - Profesional de la Oficina Asesora de Planeación **Angela Patricia Cabeza Morales** Revisión Plantilla Documental – Profesional de la Oficina Asesora de Planeación	**Carine Pening Gaviria** Líder del Macroproceso Gerencia de la Información Subsecretaría de Gestión Institucional El documento fue aprobado en sesión del Comité Institucional de Gestión y Desempeño-CIGD del 27 de enero de 2026 y publicado mediante Caso HOLA No. **24021**

1. INFORMACIÓN GENERAL

Objetivo del Plan

Definir los lineamientos y realizar las actividades necesarias para tratar de manera preventiva e integral los riesgos de Seguridad y Privacidad de la Información a los que la Secretaría Distrital de Gobierno puede estar expuesta para apoyar el cumplimiento del marco estratégico de la Entidad, por medio de la protección de la integridad, confidencialidad y disponibilidad de la información.

Responsable

Director(a) de Tecnologías e Información

Oficial Seguridad de la Información

Glosario

Activo de información: Conocimiento o información que tiene valor para el individuo u organización.

Amenazas: Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Confidencialidad: Propiedad de la información que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad autorizada.

Integridad: Propiedad de exactitud y completitud.

No repudio: Capacidad para corroborar que es cierta la reivindicación de que ocurrió un evento o una acción y las entidades que lo originaron

Riesgo de Seguridad Digital: Combinación de amenazas y vulnerabilidades en el entorno digital, puede debilitar el logro de los objetivos económicos y sociales, así como afectar la soberanía nacional la integridad territorial, el orden constitucional y los intereses nacionales, incluye aspectos relacionados con el ambiente físico, digital y las personas.

Riesgo: Efecto de la incertidumbre sobre los objetivos

Siglas

DTI: Dirección de Tecnologías e Información
ISO: Internacional Organization for Standardization) es la Organización Internacional de Normalización
MIPG: Modelo Integrado de Planeación y Gestión
MINTIC: Ministerio de Tecnologías de la Información y las Comunicaciones
TIC: Tecnologías de Información y Comunicación

2. ESTRUCTURA DEL PLAN

2.1. Introducción

En el contexto de la ciberseguridad, hoy día las organizaciones se encuentran en constante riesgo de diferentes ciber-amenazas, de tal manera que las organizaciones deben tener identificados los activos de información críticos, con el fin de dar respuestas a las partes interesadas externas e internas. Por lo anterior, la Secretaría Distrital de Gobierno construye este documento el cual tiene como objetivo dar respuesta a los objetivos estratégicos de la organización y al plan estratégico de tecnologías de la información, donde su desarrollo requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización. Adicionalmente, se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el Entorno TIC para el Desarrollo Digital, ciudadanos y hogares empoderados del Entorno Digital, Transformación Digital Sectorial y Territorial e Inclusión Social Digital.

Lo anterior dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3854 de 2016, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001, , ISO 31000:2018 y la Guía para la gestión Integral del Riesgo en Entidades Públicas Versión 7 emitida por el DAFP.

l presente documento se fundamenta en los propósitos, objetivos generales y específicos establecidos en el documento Manual de Gestión del Riesgo (PLE-PIN-M001), que se basa en la Guía para la administración del riesgo y el diseño de controles en entidades públicas. La cual contiene la metodología para el manejo de los riesgos de seguridad y privacidad de la información y la Política de Gestión de riesgo.

2.2. Objetivos específicos

- Brindar lineamientos para la gestión de los riesgos de seguridad de la información.
- Identificar, analizar, valorar y tratar los riesgos, amenazas y vulnerabilidades de seguridad digital de la Secretaría Distrital de Gobierno
- Definir las actividades requeridas para la implementar al tratamiento de riesgos de seguridad de la información.
- Evaluar el nivel de riesgo actual con el impacto generado después de implementar el plan de tratamiento de riesgos de seguridad de la información.
- Realizar seguimiento y control a la eficacia del plan de tratamiento de riesgos de seguridad de la información.

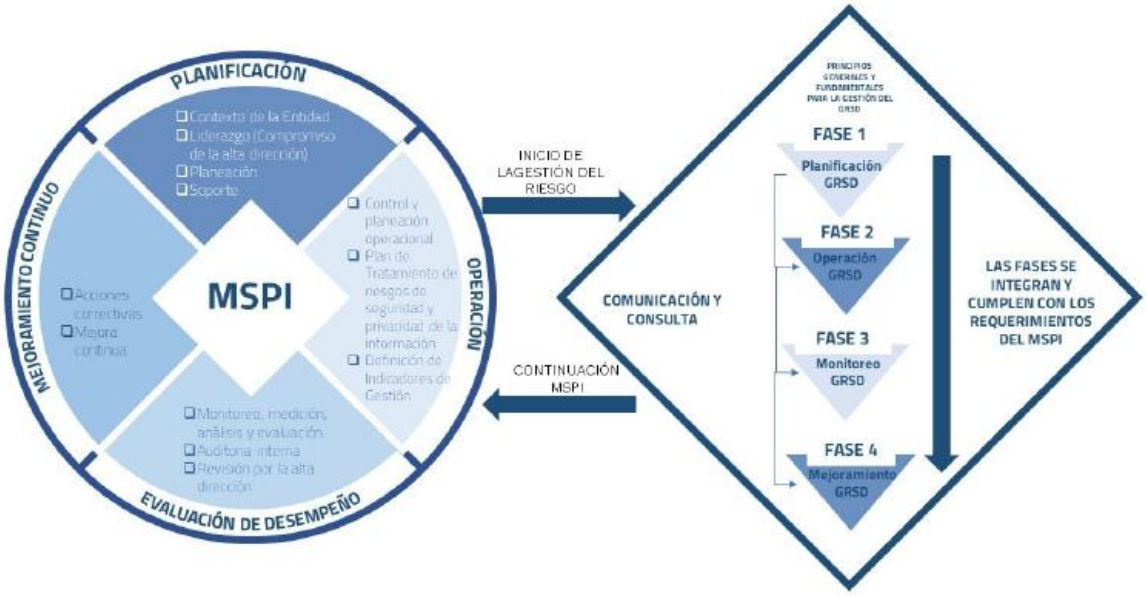
2.3. Alcance

El Plan de Tratamiento de Riesgos de Seguridad de la información tendrá en cuenta los riesgos que se identifiquen en el **Nivel Central y** en el **Nivel Local** que se encuentren en los niveles moderado, mayor y catastrófico. Las actividades que se relacionan a continuación se realizarán conforme a los manuales y procedimientos para el tratamiento de los riesgos adoptados por el sistema de gestión de la Entidad en el marco de los lineamientos del MIPG.

2.4. Política de administración del riesgo

"La Secretaría Distrital de Gobierno se compromete a identificar, analizar, valorar y monitorear los riesgos que impidan el cumplimiento de los objetivos institucionales, con el apoyo de los servidores públicos, contratistas y la participación de la ciudadanía; alcanzando las metas trazadas de manera transparente y eficaz en la gestión de los procesos, la gestión ambiental, seguridad digital y la gestión de seguridad de la información, en pro del mejoramiento continuo de la Entidad".

2.5. Marco Referencial



Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas Versión 5
Interacción MSPI - Modelo Gestión de Riesgo de seguridad de la información
Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

2.6. Desarrollo metodológico

2.6.1. Fase No 1 "planificación"

En esta fase se llevarán a cabo todas las actividades inherentes a la actualización de los lineamientos de gestión de riesgos de seguridad de la información, en concordancia con las directrices establecidas por el MINTIC y el DAFP. Asimismo, se desarrollarán acciones de capacitación y sensibilización con el propósito de fortalecer sus capacidades en la identificación, valoración y tratamiento de riesgos asociados a los activos de información, en el cual se comprenden las siguientes actividades:

- Definición del contexto interno, externo y de los procesos de la entidad pública.
- Definición de la política de administración de riesgo.

- Designación de roles y responsabilidades.
- Definición de criterios de probabilidad, impacto y zonas de riesgo aceptable.
- Identificación de activos.
- Identificación de riesgos.
- Valoración de riesgos.
- Definición del tratamiento de los riesgos.

2.6.2. Contexto externo

Para determinar el contexto externo, la Secretaría Distrital de Gobierno se consideran los siguientes factores relacionados con el entorno digital:

- Algunos de los proveedores de la entidad son Claro, UT YN2024, CamerFirma, Wexler, Solution Copy.
- Se mantiene constante relación con la Secretaría de Seguridad y Convivencia, Policía Nacional; Secretaría de Integración Social, Secretaría de la Mujer, Ministerio del Relaciones Exteriores; Consejo de Bogotá.
- Normativas o aspectos jurídicos que apliquen directa o indirectamente a la entidad pública; se encuentran consignados en el Numeral 4 "Documentos Relacionados" de este mismo documento.
- La Secretaría administra recursos asignados por el presupuesto distrital, bajo lineamientos del Decreto 411 de 2016 y la normatividad vigente. No genera ingresos propios significativos, por lo que depende de la asignación del gobierno central para cumplir sus funciones.
- La Secretaría de Gobierno contrata servicios logísticos, tecnológicos y de infraestructura con empresas privadas para ejecutar programas de participación ciudadana, seguridad y espacio público.
- El entorno cultural de la Secretaría de Gobierno frente al entorno digital se caracteriza por una transición hacia la digitalización de procesos culturales y de participación ciudadana, con el objetivo de fortalecer la transparencia, la inclusión y la interacción comunitaria.
- Cualquier otro factor externo de tipo internacional, nacional (gobierno), local.
- Los procesos electorales y cambios de gobierno para una entidad como la Secretaría de Gobierno de Bogotá son significativos porque conducen a factores externos que pueden impactar la estabilidad operativa y la seguridad digital.
- La entidad presta sus servicios a todos los ciudadanos de Bogotá D.C., los cuales son aproximadamente 7.94 millones de personas.[1]
- Ante posibles ataques cibernéticos los ciudadanos de la capital se pueden ver afectados frente a los servicios que brinda la entidad tales como certificado de residencia, certificado de propiedad horizontal, objeciones de comparendo, audiencias, respuestas a derechos de petición, tutelas, despachos comisorios, entre otros. En lo relacionado con otras entidades se podrían ver afectados la parte de comparendos con Secretaría de seguridad y convivencia, Policía Nacional y Tesorería.

1 https://telencuestas.com/censos-de-poblacion/colombia/2025/bogota

2.6.3. Contexto interno

La Secretaría Distrital de Gobierno cuenta con una estructura organizacional definida, conformada por direcciones, subdirecciones y oficinas asesoras que permiten una gestión articulada de sus funciones misionales y de apoyo. Esta estructura facilita la implementación de políticas públicas, la coordinación interinstitucional y la atención a la ciudadanía en el marco de sus competencias.

Objetivos estratégicos de la Entidad

A continuación, se presentan los objetivos estratégicos de la entidad, los cuales orientan y permiten alinear la formulación e implementación del presente Plan de Tratamiento de Riesgos de Seguridad de la Información, garantizando su coherencia con la misión institucional y el cumplimiento de las metas establecidas en el marco de la gestión pública.

- Fortalecer la identidad de ciudad mediante la comunicación estratégica y la innovación pública y social, generando cambios comportamentales y valor público.
- Fomentar la promoción, garantía, protección, respeto y apropiación de los Derechos Humanos, la Libertad Religiosa y de conciencia, el diálogo, la convivencia pacífica y la lucha contra el racismo.
- Propiciar la revolución del servicio público con criterios de calidad, calidez, eficacia, oportunidad, sostenibilidad y transformación digital.
- Fortalecer la articulación de la administración pública central y local para una gestión local y policiva más efectiva y transparente.
- Promover la transparencia, la integridad y la participación en la gestión pública, para mejorar la gobernabilidad democrática distrital y local.

Estas metas estratégicas orientan la planificación del Plan de Tratamiento de Riesgos, asegurando su coherencia con la misión institucional y su contribución al fortalecimiento del Sistema de Gestión de Seguridad de la Información (SGSI).

Por otra parte, la cultura institucional se caracteriza por el compromiso con la legalidad, la transparencia, la participación ciudadana y la mejora continua. En este sentido, la seguridad de la información se reconoce como un componente estratégico para garantizar la confianza en la gestión pública y la protección de los derechos de los ciudadanos.

En cuanto a la capacidad tecnológica, la entidad dispone de infraestructura tecnológica y de sistemas de información que soportan los procesos administrativos y misionales. No obstante, se identifican oportunidades de mejora en la actualización tecnológica, la gestión de vulnerabilidades y la implementación de controles de seguridad más robustos.

El talento humano está conformado por funcionarios públicos con perfiles técnicos y administrativos tanto en planta como contratistas, quienes desempeñan funciones clave en la operación institucional. Se reconoce la

necesidad de fortalecer las competencias en seguridad de la información, especialmente en los roles de dueños y delegados de proceso.

Los procesos internos están definidos en el marco del Modelo Integrado de Planeación y Gestión (MIPG), lo que permite una gestión orientada a resultados, con enfoque en la gestión del riesgo, la calidad y la rendición de cuentas. La identificación y tratamiento de riesgos de seguridad de la información se integran como parte fundamental de estos procesos.

En términos de recursos financieros, la entidad cuenta con un presupuesto asignado que permite la operación de sus funciones, aunque se requiere una planificación estratégica para garantizar la sostenibilidad de las acciones relacionadas con la seguridad de la información.

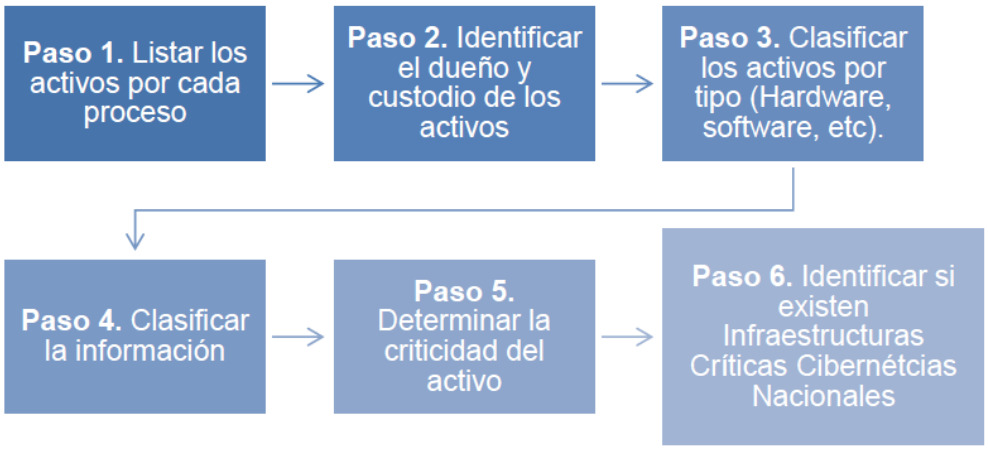
Las políticas internas en materia de seguridad de la información se encuentran en proceso de actualización, en concordancia con los nuevos lineamientos del MINTIC, el DAFP, el Esquema de Seguridad y Privacidad de la Información y la ISO/IEC-27001. Estas políticas buscan establecer un marco normativo interno que oriente la protección de los activos de información y la gestión adecuada de los riesgos asociados.

Finalmente, el marco normativo aplicable incluye la Ley 1581 de 2012 sobre protección de datos personales, la Ley 1712 de 2014 de transparencia y acceso a la información pública, el Decreto 1499 de 2017 que establece el MIPG, y las guías y lineamientos emitidos por el MINTIC en materia de seguridad digital y gobierno digital.

Identificación de activos de seguridad digital

Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital son activos elementos tales como aplicaciones de la entidad pública, servicios Web, redes, información física o digital, Tecnologías de la Información - TI que utiliza la organización para su funcionamiento. Es importante señala que la Secretaría Distrital de Gobierno ha realizado un proceso de identificación de los activos de información y documentado mediante el formato "GDI-TIC-F032 Formato identificación, valoración y clasificación de activos de información", de esta forma se identifica los activos a proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digital para interactuar con el Estado.

En la siguiente grafica se muestra los pasos adecuados para la identificación, clasificación y valoración de los activos de la Entidad:



Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025.

Identificar los riesgos inherentes de seguridad digital

De acuerdo con la metodología de gestión del riesgo de la Secretaría Distrital de Gobierno, la identificación de riesgos de seguridad digital debe realizarse siguiendo el procedimiento "*PLE-PIN-P017 Gestión de los Riesgos de Seguridad de la Información*", el cual proporciona una orientación alineada con las buenas prácticas establecidas por el MINTIC y el DAFP, garantizando un enfoque sistemático y coherente para la protección de la información institucional. :

Identificación de Amenazas:

De acuerdo con el documento del MINTIC "Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas", se presentan listados de amenazas que corresponden a situaciones o fuentes que pueden afectar los activos y materializar riesgos:

Deliberadas (D), fortuito (F), ambientales (A)

Categoria	Nº	Descripción de la amenaza	Tipo de fuente de riesgo *
Amenazas físicas	TP01	Fuego	A, D, E
	TP02	Agua	A, D, E
	TP03	Contaminación, radiación nociva	A, D, E
	TP04	Accidente grave	A, D, E
	TP05	Explosión	A, D, E
	TP06	Polvo, corrosión, heladas	A, D, E
Amenazas naturales	TN01	Fenómeno climático	E
	TN02	Fenómeno sísmico	E
	TN03	Fenómeno volcánico	E
	TN04	Fenómeno meteorológico	E
	TN05	Inundación	E
	TN06	Fenómeno de pandemia/epidemia	E
Fallas en las infraestructuras	TI01	Fallas en un sistema de suministro	A, D
	TI02	Falla del sistema de refrigeración o ventilación	A, D
	TI03	Pérdida del suministro eléctrico	A, D, E
	TI04	Falla de una red de telecomunicaciones	A, D, E
	TI05	Falla del equipo de telecomunicaciones	A, D
	TI06	Radiación electromagnética	A, D, E
	TI07	Radiación térmica	A, D, E
	TI08	Impulsos electromagnéticos	A, D, E
Fallas técnicas	TT01	Falla de dispositivos o sistemas	A
	TT02	Saturación del sistema de información	A, D
	TT03	Vulneración del mantenimiento del sistema de información	A, D
Acciones humanas	TH01	Atentado terrorista, sabotaje	D
	TH02	Ingeniería social	D
	TH03	Interceptación de la radiación de un dispositivo	D
	TH04	Espionaje remoto	D
	TH05	Escucha clandestina	D
	TH06	Robo de medios o documentos	D
	TH07	Robo de equipos	D
	TH08	Robo de identidad digital o de credenciales	D
	TH09	Recuperación de medios reciclados o descartados	D
	TH10	Divulgación de información	A, D
	TH11	Entrada de datos de fuentes no fiables	A, D
	TH12	Manipulación con hardware	D
	TH13	Manipulación con software	A, D
	TH14	Ataque de descarga oculta a través de internet	D
	TH15	Ataque de repetición, ataque de intermediario	D

Nota: Contr *pia no*

	TH16	Tratamiento no autorizado de datos personales	A, D
	TH17	Entrada no autorizada en instalaciones	D
	TH18	Uso no autorizado de dispositivos	D
	TH19	Uso incorrecto de dispositivos	A, D
	TH20	Daño de dispositivos o medios	A, D
	TH21	Copia ilícita de software	D
	TH22	Uso de software falsificado o copiado	A, D
	TH23	Corrupción de datos	D
	TH24	Tratamiento ilegal de datos	D
	TH25	Envío o distribución de malware	A, D, E
	TH26	Detección de posición	D
Compromiso de funciones o servicios	TC01	Error en el uso	A
	TC02	Abuso de derechos o permisos	A, D
	TC03	Falsificación de derechos o permisos	D
	TC04	Denegación de acciones	D
Amenazas a la organización	TO01	Falta de personal	A, E
	TO02	Falta de recursos	A, E
	TO03	Falla de los proveedores de servicios	A, E
	TO04	Violación de la legislación o la normativa	A, D
*	D : deliberado; A : accidental; E : medioambiental		

Tabla amenazas comunes
Fuente: ISO/IEC 27005:202209

Así mismo, es importante señalar que, en el proceso de identificación de riesgos, se deben considerar las tablas de referencia incluidas en el documento "Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas" del MINTIC.

- Tabla de amenazas dirigida por el hombre
- Tabla de Vulnerabilidades Comunes
- Tabla de Amenazas y Vulnerabilidades

Identificación y evaluación de controles

De acuerdo con la metodología de gestión del riesgo de la Secretaría Distrital de Gobierno, la identificación y evaluación de controles debe realizarse siguiendo el procedimiento "*PLE-PIN-P017 Gestión de los Riesgos de Seguridad de la Información*".

Tratamiento de los riesgos de seguridad digital

De acuerdo con la metodología de gestión del riesgo de la Secretaría Distrital de Gobierno, el Tratamiento de los riesgos de seguridad digital debe realizarse siguiendo el procedimiento "*PLE-PIN-P017 Gestión de los Riesgos de Seguridad de la Información*".

2.6.4. Fase No 2 Ejecución

La Dirección de Tecnologías e Información de la SDG como responsable de la seguridad digital de la entidad, realiza el acompañamiento, seguimiento al proceso de implementación de los planes de tratamiento, verificando que se ejecuten las tareas en los tiempos pactados y que los recursos se estén ejecutando de acuerdo con lo planeado.

2.6.5. Fase No 3 Monitoreo y revisión

La Secretaría Distrital de Gobierno realiza el monitoreo y la revisión del Plan de Riesgos conforme al modelo de las tres líneas de defensa definido en el MIPG, Dimensión 7 – Control Interno. En este esquema, la primera línea, conformada por los líderes de proceso, asegura la implementación y reporte de los controles; la segunda línea, a cargo de la Dirección de Tecnologías e información verifica la efectividad y genera alertas tempranas; y la tercera línea, representada por la Oficina de Control Interno, evalúa de manera independiente la eficacia del plan mediante auditorías basadas en riesgos. Este enfoque garantiza un seguimiento integral y la mejora continua en la gestión de riesgos de seguridad de la información institucionales.

Línea de Defensa	Responsable	Actividades para el seguimiento del Plan de Riesgos de Seguridad de la información
Primera Línea	Dependencias Alcaldías	Aplicar los controles definidos en el plan. Reportar avances y alertar sobre desviaciones. Documentar evidencias de implementación.
Segunda Línea	Dirección de Tecnologías e información	Monitorear la efectividad de los controles. Validar cumplimiento de actividades. Emitir recomendaciones y generar alertas tempranas.
Tercera Línea	Oficina de Control Interno	Realizar auditorías internas basadas en riesgos. Evaluar la eficacia del plan y controles. Emitir informes independientes para mejora continua.

2.6.6. Fase No 4 Mejoramiento continuo de la gestión del riesgo de seguridad digital

La Secretaría Distrital de Gobierno Garantiza la mejora continua en la gestión de riesgos de seguridad digital mediante la atención oportuna de hallazgos, falencias e incidentes, mitigando su impacto y previniendo su recurrencia, en tal sentido cuando se identifiquen hallazgos, falencias o incidentes relacionados con la seguridad digital, la Secretaría Distrital de Gobierno genera acciones inmediatas para:

- **Mitigar el impacto** de la situación detectada.
- **Controlar y corregir** la causa raíz del hallazgo o incidente.
- **Prevenir la recurrencia** mediante ajustes en procesos, controles y políticas.
- **Gestionar las consecuencias** derivadas de la no conformidad materializada, incluyendo comunicación, reporte y acciones correctivas.

2.7. Metodología para la gestión del riesgo de seguridad digital en la Secretaría Distrital de Gobierno

Las actividades planteadas para la vigencia 2026 son:

FASE	ACTIVIDAD	TAREA	RESPONSABLE	FECHA INICIO	FECHA FIN
P	Capacitación y sensibilización nivel central y local.	Capacitación y/o sensibilización en riesgos de seguridad digital	DTI - seguridad de la información	Julio 2026	Diciembre 2026
		Difusión y/o socialización de la herramienta de gestión del riesgo de seguridad digital.		Julio 2026	Diciembre 2026
H	Identificación, análisis y evaluación de riesgos de seguridad de la información en Nivel Central y Local	Identificación, análisis y evaluación de riesgos de seguridad de la información en Nivel Central y Local	DTI - seguridad de la información y dependencias y/o localidades.	Julio 2026	Diciembre 2026
H	Aceptación de los riesgos identificados y los planes de	Aprobar y publicar la matriz de riesgos de	DTI – Seguridad e la información	Julio 2026	Diciembre 2026

FASE	ACTIVIDAD	TAREA	RESPONSABLE	FECHA INICIO	FECHA FIN
	tratamiento para nivel central y local.	seguridad de la información	y dependencias y/o localidades.		
H	Realizar seguimiento de implementación de controles a los riesgos identificados para las dependencias de nivel central y local.	Realizar el seguimiento de la adopción de los controles por parte de los dueños de proceso	DTI – Seguridad e la información y dependencias y/o localidades.	Enero 2026	Diciembre 2026
V	Mejoramiento	Identificación de oportunidades en el proceso de gestión del riesgo de seguridad de la información.	DTI – Seguridad e la información	Enero 2026	Diciembre 2026
A	Monitoreo y revisión	Revisión de resultados y reporte de indicadores	DTI – Seguridad e la información	Enero 2026	Diciembre 2026

3. ESTRUCTURA DE MEDICIÓN

Metas e indicadores del Plan

Para la vigencia 2026 se plantearon las siguientes metas:

Meta	Nombre del Indicador	Fórmula del Indicador
Realizar dos (2) monitoreos de los riesgos de seguridad de la información en dependencias de Nivel Central, de las matrices de riesgos entregadas y aceptadas en la DTI durante 2025	Monitoreos realizados a dependencias de Nivel Central	Número de monitoreos realizados a dependencias de Nivel Central
Realizar dos (2) monitoreos de los riesgos de seguridad de la información, en Alcaldías Locales, de las matrices de riesgos entregada y aceptadas en la DTI durante 2025.	Monitoreos realizados a dependencias de Alcaldías Locales	Número de monitoreos realizados a dependencias de Alcaldías Locales
Acompañar a 20 Alcaldías locales en la valoración y clasificación de los	Alcaldías locales acompañadas	Número de Alcaldías locales acompañadas

riesgos de seguridad de la información de la vigencia 2026.		
Acompañar a 23 dependencias del nivel central en la construcción de la valoración y clasificación de los riesgos de seguridad de la información de la vigencia 2026.	Dependencias de nivel central acompañadas	Número de Dependencias de nivel acompañadas

Metodología de medición

Trimestral

Periodo de aplicación del plan

Vigencia 2026

4. DOCUMENTOS RELACIONADOS

Documentos internos

Código	Documento
PLE-PIN-M001	Manual de gestión del riesgo
PLE-PIN-F042	Matriz mapa de riesgos de seguridad de la información
GDI-TIC-F032	Formato de Identificación, valoración y clasificación de activos de información

Normatividad vigente

Norma	Año	Epígrafe	Artículo(s)
Ley 1341	2009	Definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnología e Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones	Toda la norma
CONPES 3701	2011	Lineamientos de Política para Ciberseguridad y Ciberdefensa.	Toda la norma
Ley 1581	2012	Disposiciones generales para la protección de datos personales	Toda la norma

Norma	Año	Epígrafe	Artículo(s)
Decreto 1078	2015	Decreto único reglamentario del sector de Tecnología e Información y las comunicaciones (define el componente de seguridad y privacidad de la información)	Toda la norma
Decreto 1081	2015	"Decreto Reglamentario Único del Sector Presidencia de la República" (En especial Libro 2)	Toda la norma
Decreto 415	2016	Por el cual 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.	Toda la norma
Resolución CDS 004	2017	Fortalecimiento Institucional en Materia de TIC, para Plan Estratégico de Tecnología y Sistemas de Información (PETI) y para la Gestión de Proyectos TIC	Toda la norma
CONPES 3854	2017	Política Nacional de Seguridad Digital	Toda la norma
Decreto 1499	2017	Modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública.	Capítulo 2
CONPES 3920	2018	Política Nacional de Explotación de datos.	Toda la norma
Resolución 783	2018	Creación del Comité Institucional de Gestión y Desempeño	Toda la norma
Decreto 1008	2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnología e Información y las Comunicaciones.	Toda la norma
Ley 1978	2019	Moderniza el sector de las Tecnología e Información y las Comunicaciones (TIC), distribuye competencias, crea	Articulo 22

Norma	Año	Epígrafe	Artículo(s)
Directiva 002	2019	un regulador único y dicta otras disposiciones. Simplificación de la interacción digital entre los ciudadanos y el estado.	Toda la norma
Generales		Lineamientos del marco de referencia establecidos por MinTIC y que incluyen Leyes, decretos y demás desarrollos normativos que guían las acciones para implementar el Marco de Referencia de Arquitectura Empresarial para la gestión de TI.	
Resolución 2277	2025	Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.	Toda la norma

Documentos externos

Nombre	Año de publicación del documento y versión	Entidad que lo emite	Medio de consulta
Ámbitos guardianes de la seguridad	2019	Alta Consejería Distrital de las TICS	http://ticbogota.gov.co/documentos/guardianes-la-informaci%c3%b3n
Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas V5	2025	MINTIC	https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/