2025

# PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA DE SALUD

## TABLA DE CONTENIDO


1 OBJETIVO ..... 1
1.1 Objetivos Específicos ..... 1
2 ALCANCE ..... 1
3 MARCO NORMATIVO ..... 1
4 DOCUMENTOS DE REFERENCIA ..... 2
5 MARCO REFERENCIAL ..... 2
5.1 Administración de Riesgos de la SDS ..... 2
5.2 Directrices del Tratamiento Riesgos ..... 2
6 ACTIVIDADES DEL PLAN ..... 3
6.1 Descripción de las Actividades ..... 3
6.2 Cronograma de Actividades ..... 4
7 INDICADORES ..... 5
8 SEGUIMIENTO ..... 5
9 ANEXOS ..... 5
10 CONTROL DE CAMBIOS ..... 6


.

# PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## 1 OBJETIVO

Implementar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información en la Secretaría Distrital de Salud de Bogotá, que garantice la adecuada identificación, análisis, tratamiento, monitoreo y mejora continua de los riesgos, asegurando la protección de los activos de información de la entidad.

### 1.1 Objetivos Específicos

- Identificar y analizar los riesgos de seguridad y privacidad de la información en los activos críticos de la Secretaría Distrital de Salud - SDS.
- Establecer medidas de tratamiento para mitigar, reducir, aceptar, evitar o transferir los riesgos detectados, alineadas con las mejores prácticas y estándares internacionales.
- Implementar de controles que minimicen las amenazas y vulnerabilidades sobre la información institucional.
- Monitorear y evaluar continuamente la efectividad de los controles implementados, asegurando su cumplimiento y mejora continua.

## 2 ALCANCE

Este plan aplica a todos los procesos, sistemas y activos de información de la Entidad, desde el establecimiento del contexto estratégico, la identificación, análisis, valoración y monitoreo, hasta la revisión y seguimiento de los riesgos de la SDS. Se centra en los riesgos moderados, altos y extremos, conforme a la metodología definida por el Departamento Administrativo de la Función Pública (DAFP) y el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

## 3 MARCO NORMATIVO

- Decreto 612 de 2018, “Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado”
- Resolución 500 de 2021. “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”.
- Resolución 1569 de 2024. “Por la cual se crea el Comité Institucional de Gestión y Desempeño y se establecen disposiciones para la operación del Modelo Integrado de Planeación y Gestión en la Secretaría Distrital de Salud de Bogotá D.C.”

# 4 DOCUMENTOS DE REFERENCIA

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

- Modelo de Seguridad y Privacidad de la Información – MinTIC, incluidos los controles basados en el Anexo A de la norma NTC ISO/IEC 27001:2013.
- Modelo Nacional de Gestión de Riesgo de Seguridad de la Información (MNGRSI) en Entidades Públicas de MinTIC.
- Modelo Nacional de Gestión de Riesgos de Seguridad Digital (MGRSD) de MinTIC
- Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas del DAFP.
- Estándar ISO/IEC 27001:2022, incluido el Anexo A.

# 5 MARCO REFERENCIAL

## 5.1 Administración de Riesgos de la SDS

Este Plan de Tratamiento se desarrolla en estricta alineación con la política, lineamientos y directrices de Administración de Riesgos establecidos por la Secretaría Distrital de Salud - SDS. El plan permite un enfoque estructurado y coherente para la gestión de riesgos, asegurando que las medidas de mitigación, control y respuesta sean consistentes con las estimaciones institucionales y contribuyan al fortalecimiento de la seguridad y resiliencia de la información dentro de la entidad.

## 5.2 Directrices del Tratamiento Riesgos

El tratamiento de riesgos consiste en la respuesta definida por la primera línea de defensa —el líder o responsable del proceso junto con su equipo de trabajo— para mitigar los diversos riesgos identificados. Esta respuesta se clasifica en las siguientes categorías:

- *Aceptar el riesgo*: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Se aclara que ningún riesgo de corrupción es aceptado). La aceptación puede resultar viable para riesgos bajos o cuando, por alguna razón, no es posible aplicar controles. En cualquiera de los casos, se requiere un seguimiento continuo para evaluar el riesgo de forma permanente.
- *Reducir el riesgo*: Se implementan medidas que disminuyen la probabilidad, el impacto o ambos; por lo general, incluyen controles adecuados y la debida segregación de funciones. De esta manera, el tratamiento del riesgo logra la reducción prevista.

- *Evitar el riesgo*: Se renuncia a las actividades que lo generan, es decir, no se inicia o no se continúa con la actividad que lo provoca.
- *Compartir el riesgo*: Se reduce la probabilidad o el impacto transfiriendo o compartiendo parte del riesgo. Aunque es posible compartir riesgos de corrupción, su responsabilidad no puede transferirse. Las dos principales vías para compartir o transferir parte del riesgo son la contratación de seguros y la tercerización.

La gestión de riesgos en Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción) permite a la SDS identificar, analizar y tratar amenazas y vulnerabilidades que puedan afectar el cumplimiento de los objetivos organizacionales. Además, contribuye a la toma de decisiones y a la prevención de la materialización de dichos riesgos.

Esta gestión considera la criticidad y nivel de protección de los activos de información de la entidad, alineándose con los objetivos, estrategias y políticas corporativas. De esta manera, se busca alcanzar un nivel de riesgo aceptable o asumible por la Alta Dirección.

## 6 ACTIVIDADES DEL PLAN

La implementación del Plan de Tratamiento requiere realizar una serie de actividades preparatorias que permitan establecer una base sólida para la gestión del riesgo en la Entidad. Estas actividades están diseñadas para comprender el contexto organizacional, identificar y evaluar los riesgos asociados a la seguridad y privacidad de la información, y definir estrategias de mitigación alineadas con la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas del DAFP, el Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas del MinTIC y la NTC ISO/IEC 27001. Este enfoque asegura que el plan sea efectivo, sostenible y responda a los desafíos específicos de la entidad en materia de seguridad digital.

### 6.1 Descripción de las Actividades

Las actividades descritas en la siguiente tabla son fundamentales para una adecuada gestión de riesgos previas al inicio del plan de tratamiento:

| ACTIVIDAD | TAREA | OBJETIVO | ACCIONES CLAVE |
|---|---|---|---|
| **Identificar, valorar y clasificar los riesgos asociados a los activos de información** | Preparación y sensibilización | Actualizar los lineamientos de Riesgos. Crear conciencia y asegurar el compromiso de los actores clave | • Formalizar el lineamiento de Riesgos de Seguridad de la información.<br>• Realizar una sensibilización sobre gestión de riesgos en seguridad y privacidad de la información con los líderes de la entidad. |

| ACTIVIDAD | TAREA | OBJETIVO | ACCIONES CLAVE |
|---|---|---|---|
| | Identificación del contexto y activos de información | Entender el entorno y determinar qué se debe proteger | • Definir el contexto interno y externo en términos de seguridad y privacidad de la información<br>• Realizar un inventario de activos de información (bases de datos, aplicaciones, documentos sensibles, infraestructura tecnológica).<br>• Clasificar los activos según su nivel de criticidad (Confidencialidad, Integridad, Disponibilidad) |
| | Identificación y evaluación de riesgos | Identificar y priorizar los riesgos en la entidad | • Determinar amenazas y vulnerabilidades para cada activo de información identificado<br>• Cuantificar el impacto y la probabilidad de ocurrencia de cada riesgo.<br>• Establecer un Mapa de Riesgos priorizando aquellos con niveles moderado, alto y extremo. |
| | Definición de estrategias de tratamiento | Determinar el manejo de los riesgos identificados | • Seleccionar estrategias de tratamiento<br>• Definir controles alineados con ISO/IEC 27001 |
| **Definir e implementar planes de tratamiento de riesgos de seguridad.** | Elaboración del Plan de Tratamiento de Riesgos | Documentar formalmente las estrategias y actividades de mitigación. | • Definir un cronograma de implementación de controles<br>• Establecer indicadores de seguimiento |
| | Implementación y monitoreo | Iniciar el plan y evaluar su efectividad. | • Realizar seguimiento y revisiones periódicas para medir la efectividad de los controles<br>• Ajustar el plan según la evolución de los riesgos y nuevas amenazas detectadas. |

La implementación de estas actividades preparatorias permite a la entidad establecer una gestión de riesgos efectiva y alineada con los marcos normativos vigentes, asegurando así la protección de la información y la continuidad operativa.

## 6.2 Cronograma de Actividades

A continuación, se presenta la planificación de las actividades a desarrollar, organizada en períodos estratégicos para su implementación

| ACTIVIDAD | TAREAS CLAVE | LIDER EJECUCION | INICIA | FINALIZA |
|---|---|---|---|---|
| **Identificar, valorar y clasificar los riesgos** | Actualización y sensibilización de lineamientos de riesgos | Equipo de gestión de riesgos | 1/2/ 2025 | 31/3/ 2025 |
| | Actualizar e identificar nuevos activos de información en cada dependencia | Gestores de procesos | 1/2/ 2025 | 31/3/ 2025 |
| | Validar, consolidar y publicar los activos de información | DPI&C, Gestión documental | 1/9/ 2025 | 15/12/ 2025 |

| ACTIVIDAD | TAREAS CLAVE | LIDER EJECUCION | INICIA | FINALIZA |
|---|---|---|---|---|
| | Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información y Seguridad Digital | Gestores de procesos | 1/5/ 2025 | 30/6/ 2025 |
| **Definir e implementar planes de tratamiento de riesgos** | Definición de planes de tratamiento de riesgos los identificados | Gestores de procesos | 1/7/ 2025 | 30/9/ 2025 |
| | Seguimiento implementación de controles | Referente de seguridad de la información (DPI&C) | 1/7/ 2025 | 31/12/ 2025 |

## 7 INDICADORES

A continuación, se presentan los indicadores seleccionados para la medición del desempeño de este plan.

| ACTIVIDAD | INDICADOR | META |
|---|---|---|
| **Identificar, valorar y clasificar los riesgos** | Porcentaje de activos de información evaluados en la matriz de riesgos. | 100% de los activos de información registrados en la matriz de riesgos. |
| **Definir e implementar planes de tratamiento de riesgos** | Porcentaje de riesgos con planes de tratamiento implementados. | 90% de los riesgos críticos con planes de tratamiento implementados. |

## 8 SEGUIMIENTO

A continuación, se presentan los mecanismos y herramientas utilizados para el seguimiento y control del plan.

| ACTIVIDAD | SEGUIMIENTO | RESPONSABLE |
|---|---|---|
| **Identificar, valorar y clasificar los riesgos** | Evaluación semestral de la matriz de riesgos y actualización de registros. | Líder de Gestión de Riesgos / Referente de seguridad de la información (DPI&C). |
| **Definir e implementar planes de tratamiento de riesgos** | Seguimiento bimensual a la implementación de los planes de tratamiento de riesgos. | Líder de Gestión de Riesgos, Gestores de cada proceso |

## 9 ANEXOS

Guía para la Administración del Riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública (DAFP) https://www.funcionpublica.gov.co/documents/28587410/34299967/Guia_administracion_riesgos_capitulo_riesgo_fiscal.pdf

El Modelo de Seguridad y Privacidad de la Información, el cual puede ser consultado en línea y descargar las guías pertinentes, en la dirección: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

Los lineamientos y estándares para la estrategia de seguridad digital y el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital pueden ser consultados en línea y descargar las guías pertinentes, en la dirección: https://normograma.mintic.gov.co/mintic/compilacion/docs/resolucion_mintic_0500_2021.htm

## 10 CONTROL DE CAMBIOS

| VERSIÓN | FECHA DE APROBACIÓN | RAZÓN DE ACTUALIZACIÓN | CRÉDITOS |
|---|---|---|---|
| 1 | 31/01/2025 | Se crea con el propósito establecer el tratamiento de los riesgos de información y los activos digitales respondiendo a la necesidad de cumplir con normativas vigentes. | Luis Guillermo Barrera |