Plan Tratamiento de Riesgos de Seguridad de la Información

2026

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

1. Introducción

La información constituye uno de los activos más estratégicos de la Secretaría Distrital de Salud, dado que soporta la toma de decisiones, la prestación de servicios esenciales y la confianza de la ciudadanía en la gestión institucional; En un entorno caracterizado por la transformación digital, la interconexión de sistemas y la creciente sofisticación de las amenazas cibernéticas, la protección de los datos personales, sensibles y misionales se convierte en un imperativo para garantizar la continuidad operativa y la seguridad de los procesos, que permiten reconocer la información como un activo estratégico e implica asumir que su valor trasciende lo técnico y se proyecta hacia lo legal, lo organizacional y lo social, siendo indispensable establecer mecanismos de gestión que aseguren su confidencialidad, integridad y disponibilidad.

Este Plan de Tratamiento de Riesgos y Seguridad de la Información se fundamenta en un marco normativo robusto que integra estándares internacionales y disposiciones nacionales, en el ámbito global, se adoptan las directrices de la norma ISO/IEC 27001 de 2022, que establece los requisitos para implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI), y la norma ISO 31000 de 2018, que define los principios y directrices para la gestión integral de riesgos, también se incorpora el Modelo de Seguridad y Privacidad de la Información (MSPI), como referente nacional que articula la política pública de seguridad digital con las prácticas de gestión institucional.

En el contexto colombiano, este plan se alinea con la Ley 1581 de 2012 sobre protección de datos personales, el Decreto 1377 de 2013 que reglamenta su aplicación, el Decreto 1078 de 2015 que consolida las disposiciones del sector TIC, y la Resolución 500 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones, que adopta lineamientos específicos para la seguridad digital en entidades públicas.

De igual manera, se consideran los documentos CONPES 3854 de 2016 y CONPES 3995 de 2021, que establecen la política nacional de seguridad digital y de ciberseguridad, respectivamente, como instrumentos de referencia para fortalecer las capacidades institucionales frente a riesgos emergentes.

La alineación con estas políticas nacionales e internacionales asegura que el presente plan no solo responda a las necesidades internas de la Secretaría Distrital de Salud, sino que también se articule con los compromisos del estado colombiano en materia de seguridad digital, protección de datos y confianza ciudadana, por lo que de esta manera, se garantiza que la gestión de riesgos de seguridad de la información se realice bajo criterios de trazabilidad, legalidad y mejora continua, consolidando un marco de actuación que permita enfrentar los desafíos actuales y futuros con rigor técnico y respaldo normativo.

2. Contexto institucional y diagnóstico

La Secretaría Distrital de Salud enfrenta un entorno digital cada vez más complejo, caracterizado por la acelerada transformación tecnológica, la interconexión de sistemas de información y la creciente sofisticación de las amenazas cibernéticas, en este escenario,

los riesgos asociados a la seguridad y privacidad de la información se convierten en factores críticos que pueden comprometer la continuidad de los servicios prestados por la secretaría Distrital de Salud, la confianza de los ciudadanos y el cumplimiento normativo.

Entre los principales riesgos actuales se destacan los ciberataques dirigidos a infraestructuras críticas, la fuga de datos sensibles relacionados con información y registros administrativos y la interrupción de servicios esenciales ocasionada por incidentes tecnológicos o ataques de denegación de servicio, estos riesgos, de materializarse, no solo afectan la operatividad institucional, sino que también generan impactos legales, reputacionales y sociales de gran magnitud.

El diagnóstico institucional evidencia que la protección de la información en el sector salud requiere un enfoque integral que combine medidas técnicas, organizativas y legales ya que la creciente dependencia de plataformas digitales para la gestión de información de las diferentes áreas, la interoperabilidad de sistemas y la prestación de servicios en línea amplifica la exposición a vulnerabilidades, por ello, resulta indispensable contar con un plan de tratamiento de riesgos que permita anticipar escenarios de amenaza, establecer controles efectivos y garantizar la resiliencia organizacional frente a incidentes de seguridad.

La formulación de este plan se nutre de las experiencias previas de la entidad que ha avanzado en la implementación de modelos de gestión de riesgos de seguridad digital donde el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) ha establecido lineamientos estratégicos a través del Modelo de Seguridad y Privacidad de la Información (MSPI) y la Resolución 500 de 2021, que sirven como referentes normativos y metodológicos, han incorporado la gestión de riesgos en su marco institucional, articulando políticas de seguridad digital con el Modelo Integrado de Planeación y Gestión (MIPG).

La referencia a estas experiencias permite a la Secretaría Distrital de Salud adoptar buenas prácticas, ajustar metodologías y consolidar un enfoque normativo y técnico que garantice la protección de la información en el ámbito de la salud pública digital, de esta manera, el diagnóstico institucional no solo identifica los riesgos prioritarios, sino que también establece un marco de aprendizaje y adaptación que fortalece la capacidad de gestión de riesgos de la entidad en la vigencia 2026.

3. Objetivos

Objetivo general:

El Plan de Tratamiento de Riesgos y Seguridad de la Información de la Secretaría Distrital de Salud para la vigencia 2026 es garantizar la confidencialidad, integridad y disponibilidad de la información institucional. Estos tres principios fundamentales constituyen la base de la gestión de seguridad de la información y aseguran que la información y los datos privados y sensibles de la entidad, en especial aquellos relacionados con la atención ciudadana, se mantengan protegidos frente a amenazas internas y externas.

La confidencialidad busca impedir accesos no autorizados, la integridad asegura que la información no sea alterada de manera indebida, y la disponibilidad garantiza que los sistemas y servicios estén accesibles cuando se requieran para la operación misional.

Por lo que se describen los siguientes objetivos específicos:

1. Primero consiste en fortalecer la infraestructura tecnológica mediante la implementación de controles técnicos avanzados, la modernización de plataformas digitales y la adopción de arquitecturas seguras que soporten la gestión de datos sensibles, ya que este fortalecimiento se orienta a reducir vulnerabilidades y a incrementar la resiliencia institucional frente a incidentes de seguridad.
2. Cumplir con la normativa vigente, tanto nacional como internacional, asegurando la alineación con estándares como ISO/IEC 27001 de 2022 e ISO 31000 de 2018, así como con la legislación colombiana en materia de protección de datos personales y seguridad digital, porque este cumplimiento normativo no solo garantiza la legalidad de las actuaciones institucionales, sino que también refuerza la confianza de los ciudadanos y de los órganos de control en la gestión de la Secretaría Distrital de Salud.
3. Se deberá establecer un sistema de monitoreo continuo de riesgos, que permita identificar, evaluar y dar seguimiento a las amenazas emergentes y a la efectividad de los controles implementados, en este sistema debe incluir indicadores de desempeño y mecanismos de retroalimentación que aseguren la mejora continua del proceso de gestión de riesgos.
4. Fomentar una cultura organizacional de ciberseguridad, promoviendo la sensibilización y capacitación de los funcionarios y contratistas en buenas prácticas de seguridad digital.

La construcción de esta cultura es esencial para que la gestión de riesgos trascienda lo técnico y se convierta en un compromiso colectivo, donde cada miembro de la entidad asuma la responsabilidad de proteger la información y contribuir a la resiliencia institucional.

En conjunto, estos objetivos proporcionan un marco estratégico que articula la protección de la información con la misión institucional de la Secretaría Distrital de Salud, asegurando que la gestión de riesgos se realice con rigor técnico, respaldo normativo y enfoque preventivo.

Además de los objetivos ya definidos, el Plan de Tratamiento de Riesgos y Seguridad de la Información para la Secretaría Distrital de Salud en la vigencia 2026 incorpora objetivos complementarios que fortalecen la gestión integral de la seguridad digital y la resiliencia institucional, ya que estos objetivos adicionales buscan ampliar el alcance del plan, garantizar su sostenibilidad en el tiempo y consolidar una cultura organizacional orientada a la protección de la información.

Objetivos generales adicionales:

- Consolidar la resiliencia institucional frente a incidentes de seguridad digital**,** asegurando que la entidad pueda responder de manera efectiva y recuperar la operación en tiempos mínimos ante eventos disruptivos.
- Integrar la gestión de riesgos de seguridad de la información con la planeación estratégica institucional, de manera que las decisiones de alto nivel consideren la protección de los activos digitales como un eje transversal.
- Fortalecer la confianza ciudadana en el manejo de la información pública y sensible, garantizando transparencia, trazabilidad y cumplimiento de los principios de protección de datos personales.
- Desarrollar protocolo de respuesta a incidentes de seguridad, alineado con estándares internacionales y normatividad nacional, que incluyan procedimientos claros de detección, contención, análisis y recuperación.
- Implementar mecanismos de trazabilidad documental, que permitan demostrar ante órganos de control la correcta gestión de riesgos y la efectividad de los controles aplicados.
- Promover la interoperabilidad segura de sistemas de información, asegurando que el intercambio de datos entre entidades se realice bajo estándares de seguridad y privacidad.
- Incorporar indicadores de madurez en la gestión de riesgos, que midan la evolución de la entidad en la implementación de controles, la reducción de vulnerabilidades y la mejora continua del SGSI.
- Impulsar programas de formación especializada en ciberseguridad para funcionarios y contratistas, con el fin de elevar las competencias técnicas y fortalecer la capacidad institucional de prevención y respuesta.
- Adoptar tecnologías emergentes de protección de la información, como soluciones de inteligencia artificial para detección de anomalías, cifrado avanzado y gestión automatizada de accesos.

En conjunto, estos objetivos adicionales complementan los ya establecidos y permiten que el plan evolucione hacia un modelo más robusto, preventivo y sostenible, capaz de enfrentar los desafíos de la seguridad digital y de responder con eficacia a las exigencias normativas y sociales del año 2026.

4. Alcance

El Plan de Tratamiento de Riesgos y Seguridad de la Información de la Secretaría Distrital de Salud (SDS) para la vigencia 2026 se aplica de manera integral a todos los procesos institucionales, abarcando tanto las funciones misionales como las actividades administrativas, de apoyo y de soporte tecnológico, ya que en el ámbito misional, el plan cubre los sistemas de información, la gestión de datos e información y la administración de programas de salud pública, garantizando que los datos sensibles de los ciudadanos se mantengan protegidos frente a amenazas internas y externas; ya en el ámbito administrativo, se incluyen los procesos de planeación, gestión financiera, talento humano

y contratación, reconociendo que la seguridad de la información es transversal y afecta directamente la eficiencia y la transparencia institucional.

En el componente tecnológico, el alcance se extiende a la infraestructura de redes, servidores, aplicaciones, plataformas digitales y dispositivos que soportan la operación de la SDS, lo que implica la implementación de controles técnicos y organizativos que aseguren la disponibilidad de los servicios digitales, la integridad de los sistemas y la confidencialidad de los datos procesados, la cobertura tecnológica también contempla la interoperabilidad con sistemas externos, la gestión de accesos y la protección de entornos de nube, considerando las mejores prácticas definidas en las normas ISO/IEC 27001 de 2022 y ISO 31000 de 2018, así como en el Modelo de Seguridad y Privacidad de la Información (MSPI).

De manera complementaria, el plan incluye la participación de terceros y proveedores de servicios digitales que tengan acceso a los activos de información institucional, que también a abarca contratistas, operadores tecnológicos, aliados estratégicos y cualquier entidad externa que preste servicios relacionados con la gestión de datos o el soporte digital, para que la inclusión de estos actores responde a la necesidad de establecer responsabilidades compartidas y mecanismos de control que aseguren que las medidas de seguridad se apliquen de manera uniforme en toda la cadena de valor, en este sentido, se exige que los proveedores cumplan con la normativa nacional vigente en materia de protección de datos personales, así como con los estándares internacionales de seguridad de la información, garantizando la trazabilidad y la legalidad de las operaciones.

En conclusión, el alcance del plan es amplio y transversal, asegurando que la gestión de riesgos de seguridad de la información se aplique de manera coherente en todos los niveles de la Secretaría Distrital de Salud y en las relaciones con terceros; este enfoque integral permite consolidar un sistema de protección robusto, capaz de responder a los desafíos de la salud pública digital y de garantizar la confianza de los ciudadanos en la gestión institucional.

5. Marco normativo

El Plan de Tratamiento de Riesgos y Seguridad de la Información de la Secretaría Distrital de Salud hace que este marco constituya la base para la implementación de controles, la definición de responsabilidades.

En el ámbito internacional, la norma ISO/IEC 27001 de 2022 establece los requisitos para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), orientado a preservar la confidencialidad, integridad y disponibilidad de los activos de información, su enfoque basado en riesgos permite identificar amenazas, evaluar vulnerabilidades y aplicar controles proporcionales a la criticidad de los procesos institucionales.

Complementariamente, la ISO 31000 de 2018 proporciona principios y directrices para la gestión integral de riesgos, promoviendo un enfoque sistemático y estructurado que facilita

la toma de decisiones y la mejora continua, este Modelo de Seguridad y Privacidad de la Información (MSPI), desarrollado en Colombia, articula estas buenas prácticas internacionales con la política pública de seguridad digital, ofreciendo lineamientos específicos para entidades públicas en materia de protección de datos y gestión de riesgos tecnológicos.

En el contexto nacional, el plan se alinea con la Ley 1581 de 2012**,** que regula la protección de datos personales y establece principios como legalidad, finalidad, libertad, veracidad y seguridad en el tratamiento de la información, en el Decreto 1377 de 2013 complementa esta ley, definiendo procedimientos para la autorización y manejo de datos sensibles, por su parte, el Decreto 1078 de 2015, como Decreto Único Reglamentario del sector TIC, consolida las disposiciones relacionadas con la seguridad digital y la gestión de la información en entidades públicas, la Resolución 500 de 2021 del MinTIC adopta lineamientos específicos para la estrategia de seguridad digital y fortalece el MSPI como habilitador de la Política General de Seguridad de la Información.

Finalmente, los documentos CONPES 3854 de 2016 y CONPES 3995 de 2021 constituyen referentes estratégicos de política pública:

1. Establece la Política Nacional de Seguridad Digital, orientada a fortalecer las capacidades institucionales para identificar, gestionar y mitigar riesgos en el entorno digital.
2. Define la Política Nacional de Ciberseguridad y Confianza Digital, enfocada en la protección de infraestructuras críticas, la gestión de incidentes y la promoción de la confianza ciudadana en el uso de servicios digitales.

La integración de este marco normativo asegura que el Plan de Tratamiento de Riesgos y Seguridad de la Información de la Secretaría Distrital de Salud se ejecute bajo criterios de legalidad, trazabilidad y mejora continua, para que asimismo garantice que las acciones emprendidas por la SDS, estén alineadas con las mejores prácticas internacionales y con las políticas nacionales de seguridad digital, consolidando un sistema de gestión robusto y preparado para enfrentar los desafíos de la vigencia 2026.

6. Metodología de gestión de riesgos

La metodología adoptada por la Secretaría Distrital de Salud para la gestión de riesgos de seguridad de la información se fundamenta en el ciclo establecido por la norma ISO 31000 de 2018, el cual proporciona un enfoque estructurado, sistemático y adaptable para la administración de riesgos en organizaciones públicas y privadas donde este ciclo permite garantizar que la gestión de riesgos se realice de manera coherente, trazable y alineada con los objetivos institucionales, integrando tanto los aspectos técnicos como los organizativos y legales.

6.1. Establecimiento del contexto

En esta fase se determina el marco de referencia que orientará la gestión de riesgos de seguridad de la información, se definen los objetivos estratégicos alineados con las políticas institucionales, el alcance del proceso de gestión y los criterios de evaluación que servirán como parámetros para la identificación, análisis y tratamiento de riesgos.

Asimismo, se lleva a cabo la identificación y clasificación de los activos de información críticos, los procesos misionales y de apoyo administrativo, así como las dependencias tecnológicas que garantizan la continuidad operativa de la secretaría, para que el ejercicio permita establecer una visión integral de los elementos esenciales necesarios para la gestión de riesgos y asegurando que la gestión de estos se realice con base en la relevancia, sensibilidad y valor institucional de cada activo.

La definición del contexto constituye el fundamento para la trazabilidad y la efectividad del proceso, asegurando que las decisiones adoptadas en materia de seguridad y privacidad estén sustentadas en criterios objetivos, normativos y estratégicos que fortalezcan la resiliencia institucional frente a amenazas y vulnerabilidades.

6.2. Identificación de Riesgos

La identificación de riesgos constituye una etapa crítica dentro del proceso de gestión de seguridad de la información, orientada a reconocer de manera detallada y sistemática las amenazas potenciales y las vulnerabilidades que pueden afectar la integridad, disponibilidad y confidencialidad de los activos de información y activos tecnológicos institucionales.

Este paso se fundamenta en la elaboración y mantenimiento de inventarios actualizados de sistemas de información y equipos tecnológicos, bases de datos, aplicaciones y servicios digitales que soportan la operación misional y administrativa de la secretaría. Asimismo, se integra la revisión de incidentes de seguridad ocurridos en periodos anteriores, con el fin de extraer lecciones aprendidas y fortalecer la capacidad de anticipación frente a eventos similares.

Utilizando los siguientes formatos destinados para tal fin:

- Matriz de Riesgos: Tabla estructurada con columnas de *activo, amenaza, vulnerabilidad, probabilidad, impacto, nivel de riesgo*; ya que es fácil de actualizar, exportar y graficar en mapas de calor.
- Ficha Técnica de Riesgo: Documento que describe cada riesgo con detalle: identificación, responsable, controles existentes, controles propuestos, indicadores de seguimiento, al ser utilizado se asegura trazabilidad documental y cumplimiento normativo.

6.3 Análisis de riesgos

La fase de análisis de riesgos constituye un componente esencial dentro del proceso de gestión de seguridad de la información, ya que permite evaluar de manera estructurada la probabilidad de ocurrencia de cada amenaza y el impacto potencial que podría generar sobre los activos institucionales en caso de materializarse.

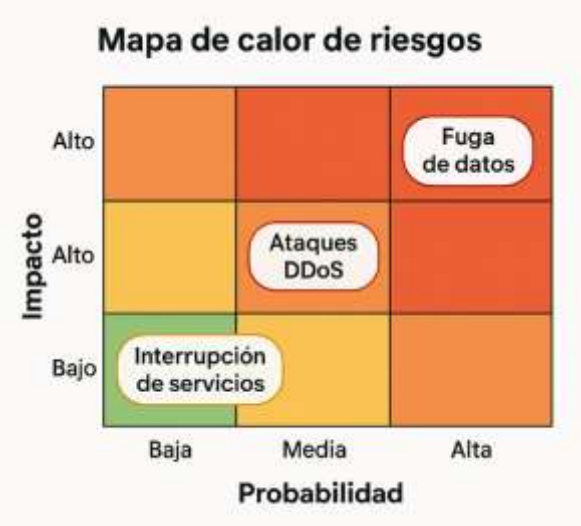
Este análisis se desarrolla mediante metodologías reconocidas de evaluación de riesgos, que integran criterios cuantitativos y cualitativos para determinar el nivel de exposición de la entidad, donde los resultados obtenidos permiten clasificar los riesgos en niveles de criticidad (bajo, medio, alto y crítico), facilitando la priorización de acciones de tratamiento y la asignación eficiente de recursos destinados para la seguridad.

La clasificación de riesgos se fundamenta en la valoración de factores como:

- Impacto en la operación misional y administrativa: considerando la continuidad en las áreas.
- Sensibilidad y valor de la información: especialmente en lo relacionado con la información, activos de información y tecnológicos y datos personales.
- Dependencia tecnológica: en términos de infraestructura, aplicaciones y servicios digitales críticos.
- Cumplimiento normativo: respecto a la legislación vigente en materia de protección de datos y seguridad de la información.

De esta manera, el análisis de riesgos proporciona una base objetiva y trazable para la toma de decisiones estratégicas, asegurando que las medidas de mitigación y control se orienten hacia los escenarios de mayor relevancia y que el tratamiento de riesgos fortalezca la resiliencia institucional frente a amenazas emergentes y persistentes.

El mapa de calor de riesgos permite visualizar de manera clara la relación entre la probabilidad de ocurrencia y el impacto potencial de cada amenaza, ya que los riesgos ubicados en el cuadrante rojo (crítico) requieren atención inmediata y recursos prioritarios, mientras que los riesgos en amarillo y naranja deben ser gestionados con medidas de mitigación proporcionales y en ese análisis, la fuga de datos se clasifica como crítico, los ataques DDoS como alto y la interrupción de servicios como medio.



Grafica Mapa de Calor

6.4 Evaluación de Riesgos

Es el punto de convergencia entre el análisis realizado y los criterios institucionales previamente establecidos, para proceder a comparar los resultados obtenidos respecto a la probabilidad e impacto de cada riesgo con los parámetros definidos en las políticas de seguridad y privacidad de la información, así como con los estándares normativos.

El objetivo principal es determinar el nivel de aceptabilidad de los riesgos identificados, diferenciando aquellos que pueden ser asumidos por la organización sin comprometer la operación misional, de aquellos que requieren acciones inmediatas de mitigación, control o transferencia, esta valoración permite priorizar la asignación de recursos y establecer planes de tratamiento proporcionales al nivel de criticidad de cada escenario.

La evaluación se fundamenta en criterios como:

- **Cumplimiento normativo y regulatorio**: En relación con la legislación vigente en materia de protección de datos y seguridad de la información.
- **Impacto en la continuidad**: Considerando la criticidad de los procesos asistenciales y administrativos.
- **Sensibilidad de la información comprometida**: Especialmente en lo referente a datos personales, privados y sensibles.
- **Capacidad institucional de respuesta:** En términos de recursos tecnológicos, humanos y financieros disponibles.

De esta manera, la evaluación de riesgos asegura que las decisiones adoptadas sean objetivas, trazables y alineadas con los objetivos estratégicos de la Secretaría de Salud,

fortaleciendo la resiliencia institucional frente a amenazas emergentes y garantizando la protección integral de la información crítica.

6.5 Tratamiento de Riesgos

La fase de tratamiento de riesgos constituye el momento en el que la organización define y ejecuta las acciones necesarias para gestionar los riesgos previamente evaluados, asegurando que las decisiones adoptadas estén alineadas con los objetivos estratégicos y normativos de la Secretaría de Salud.

Este proceso implica la selección, diseño e implementación de medidas específicas orientadas a mitigar, transferir, aceptar o evitar los riesgos identificados, de acuerdo con su nivel de criticidad y el impacto potencial sobre los activos de información y los procesos misionales.

Las medidas de tratamiento se estructuran en tres dimensiones complementarias:

- **Técnicas:** Controles de acceso, mecanismos de autenticación robusta, cifrado de datos en tránsito y reposo, monitoreo continuo de redes y sistemas, gestión de vulnerabilidades y aplicación de parches de seguridad.
- **Organizativas:** Socialización y actualización de políticas institucionales, procedimientos operativos estandarizados, programas de capacitación y concienciación del personal, así como la asignación clara de roles y responsabilidades en materia de seguridad de la información.
- **Legales y normativas:** Alineación con la legislación vigente en protección de datos personales, cumplimiento de estándares internacionales de seguridad y privacidad, y adopción de cláusulas contractuales que aseguren la responsabilidad compartida con terceros proveedores de servicios tecnológicos.

El tratamiento de riesgos debe ser documentado, trazable y medible, garantizando que cada acción implementada cuente con indicadores de eficacia y mecanismos de seguimiento que permitan evaluar su impacto en la reducción de la exposición institucional, de esta manera, se fortalece la recuperación y resiliencia organizacional frente a amenazas emergentes y se asegura la protección integral de la información crítica para la prestación de los servicios de salud.

6.6 Monitoreo y Revisión

La fase de monitoreo y revisión constituye el mecanismo que asegura la mejora continua del sistema de gestión de riesgos de seguridad de la información, en esta etapa se implementan procesos sistemáticos de seguimiento, evaluación y retroacción que permiten verificar la eficacia de los controles establecidos y garantizar su alineación con los objetivos estratégicos de la secretaría.

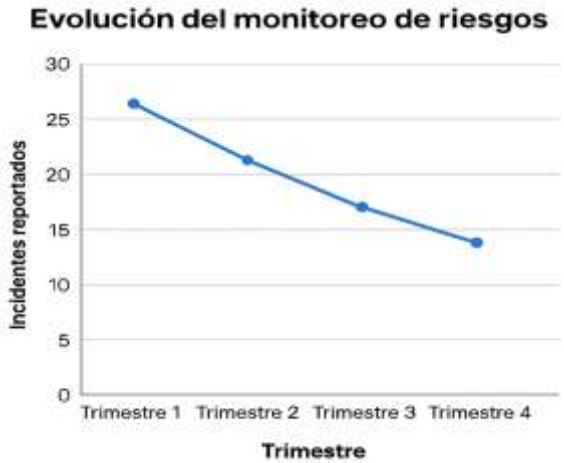
El monitoreo se materializa a través de revisiones periódicas de cumplimiento normativo y la aplicación de indicadores de desempeño que midan la efectividad de las medidas de seguridad, porque estos ejercicios permiten identificar desviaciones, brechas o nuevas vulnerabilidades, generando insumos para la toma de decisiones oportunas y fundamentadas.

La revisión, por su parte, implica la actualización continua de las matrices de riesgos, considerando los cambios en el entorno tecnológico, normativo y organizacional, así como la aparición de nuevas amenazas y escenarios críticos para el sector salud, donde este proceso asegura que la gestión de riesgos se mantenga vigente, trazable y adaptable frente a la evolución del contexto institucional.

De esta manera, el monitoreo y la revisión consolidan un ciclo de mejora continua que fortalece la resiliencia organizacional, garantizando que las medidas de seguridad y privacidad respondan de manera efectiva a los desafíos emergentes y contribuyan a la protección integral de los activos tecnológicos y activos de información y la continuidad de las actividades misionales y operativas.

Para apoyar este ciclo, la Secretaría Distrital de Salud utiliza herramientas como matrices de riesgos, que permiten documentar amenazas, vulnerabilidades, consecuencias y controles asociados; los mapas de calor, que facilitan la visualización de la criticidad de los riesgos en función de su probabilidad e impacto y los registros de controles, que aseguran la trazabilidad y la evidencia documental de las medidas aplicadas. Estas herramientas fortalecen la capacidad institucional de anticipar escenarios de riesgo, priorizar acciones.

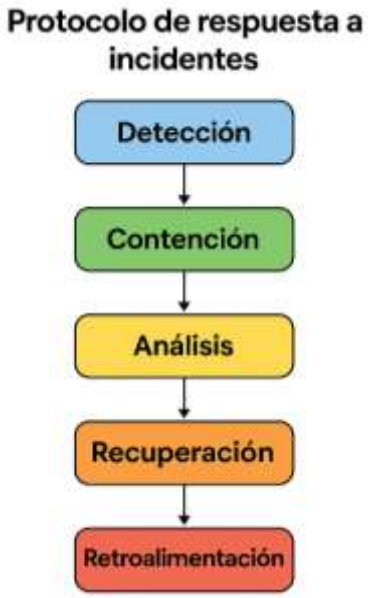
En conjunto, la metodología de gestión de riesgos aplicada garantiza que la Secretaría Distrital de Salud cuente con un sistema robusto, normativamente alineado y técnicamente sustentado, capaz de proteger sus activos tecnológicos y de información y asegurar la continuidad de los servicios críticos de salud en la vigencia 2026.



Evolución del monitoreo de riesgos

7. Actividades de Gestión de Riesgos

La gestión de riesgos de seguridad de la información en la Secretaría Distrital de Salud se articula mediante un conjunto de actividades estratégicas que garantizan la identificación, evaluación, tratamiento y monitoreo de las amenazas que puedan comprometer la operación institucional y la protección de los activos críticos. Estas actividades se desarrollan bajo un enfoque normativo y técnico, alineado con los estándares internacionales ISO/IEC 27001 de 2022 e ISO 31000 de 2018, así como con el Modelo de Seguridad y Privacidad de la Información (MSPI)**,** asegurando trazabilidad, cumplimiento regulatorio y mejora continua.



7.1. Inventario de Activos de Información

El inventario de activos constituye la base para la gestión de riesgos, este debe ser exhaustivo, actualizado periódicamente y abarcar sistemas de información, bases de datos, aplicaciones, infraestructura tecnológica y procesos misionales, esta clasificación de los activos según su criticidad, sensibilidad y valor institucional permite priorizar aquellos que requieren mayores niveles de protección y controles específicos, garantizando la adecuada asignación de recursos de seguridad.

7.2. Actualización de la Matriz de Riesgos

La matriz de riesgos integra amenazas, vulnerabilidades y consecuencias asociadas a los activos identificados, y se construye con criterios de probabilidad e impacto, lo que facilita la determinación del nivel de riesgo y la definición de acciones de tratamiento, su actualización periódica asegura la incorporación de riesgos emergentes derivados de

cambios tecnológicos, regulatorios o del entorno, manteniendo vigente y pertinente el análisis institucional.

7.3. Monitoreo de Controles

El monitoreo de controles permite evaluar la efectividad de las medidas implementadas para mitigar los riesgos y se realiza mediante revisiones sistemáticas y verificación de evidencias documentales, garantizando la trazabilidad de las acciones emprendidas, los resultados obtenidos sirven para ajustar los controles, reforzar aquellos que presentan debilidades y consolidar la capacidad institucional de respuesta frente a incidentes.

7.4. Capacitación y Sensibilización del Personal

La formación continua y la sensibilización del personal constituyen un eje fundamental para consolidar una cultura organizacional de ciberseguridad, donde las capacitaciones en buenas prácticas de seguridad digital, protección de datos personales y gestión de riesgos fortalecen las competencias de funcionarios y contratistas, asegurando que cada actor institucional asuma su responsabilidad en la protección de la información y en la resiliencia de los procesos misionales.

7.5. Evaluar normalización y calidad desarrollos en aplicaciones.

La evaluación de la normalización y calidad en los desarrollos de aplicaciones constituye un componente estratégico dentro de la gestión de riesgos de seguridad de la información, dado que las aplicaciones institucionales son el medio principal para el procesamiento, almacenamiento y transmisión de datos sensibles y misionales y la ausencia de estándares claros en el ciclo de desarrollo puede generar vulnerabilidades críticas, comprometer la interoperabilidad de sistemas y afectar la operación y la trazabilidad de los procesos.

Normalización de procesos de desarrollo:

- Contar con Arquitecto de desarrollo.
- Aplicación de metodologías reconocidas como *DevSecOps*, *Agile* o *Scrum*, integrando controles de seguridad desde la fase de diseño.
- Uso de estándares de codificación segura para prevenir vulnerabilidades comunes como inyecciones SQL, XSS o fallos de autenticación.
- Documentación técnica y funcional que asegure trazabilidad y cumplimiento normativo.

Calidad de los desarrollos:

- Implementación de pruebas de calidad (QA/QC) que incluyan pruebas unitarias, de integración, de seguridad y de rendimiento.

- Validación de requisitos funcionales y no funcionales, garantizando que las aplicaciones cumplan con los objetivos misionales y con los principios de confidencialidad, integridad y disponibilidad.
- Auditorías de código y revisiones periódicas para detectar errores, malas prácticas o dependencias inseguras.

Impacto organizativo y normativo:

- La calidad en los desarrollos asegura la resiliencia institucional, evitando interrupciones en servicios críticos de salud.
- La normalización permite cumplir con marcos regulatorios como la Ley 1581 de 2012 (protección de datos personales), la Resolución 500 de 2021 del MinTIC y estándares internacionales como ISO/IEC 27001 **e** ISO 31000.
- La evaluación periódica de aplicaciones fortalece la confianza ciudadana y la capacidad de defensa institucional.

Gestión de riesgos asociados:

- Riesgo de **fuga de datos** por aplicaciones mal diseñadas.
- Riesgo de **interrupción de servicios** por fallos de calidad en el software.
- Riesgo de **incumplimiento normativo** por ausencia de estándares de seguridad en el desarrollo.

Atención en el desarrollo frente Seguridad de la Información

Permite asegurar que la evaluación de aplicaciones no se limite a aspectos funcionales o normativos, sino que también aborde de manera proactiva las vulnerabilidades técnicas que podrían comprometer la operación misional, la protección de datos personales y el cumplimiento legal.

- Análisis de vulnerabilidades: ejecución de escaneos periódicos en aplicaciones y servidores para identificar brechas y fallos de seguridad.
- Pruebas de penetración (Pentesting): simulación de ataques controlados para evaluar la resistencia de las aplicaciones frente a amenazas reales.
- Gestión de brechas: clasificación de vulnerabilidades según criticidad (baja, media, alta, crítica) y definición de planes de remediación.
- Indicadores de seguridad: métricas que midan la reducción de brechas, tiempos de respuesta y efectividad de los controles aplicados.
- Retroalimentación continua: integración de hallazgos en el ciclo de desarrollo para fortalecer la resiliencia institucional y evitar reincidencias.

Tabla de riesgos de seguridad de la información

Para las actividades se deberá utilizar la Matriz de Identificación y Clasificación de Riesgos de Seguridad de la Información ya que usarla garantiza que la gestión de riesgos no sea

subjetiva ni dispersa, sino estructurada y medible, además que es la base para construir planes de tratamiento, protocolos de respuesta y controles efectivos.

La tabla de riesgos de seguridad de la información no debe entenderse únicamente como un inventario de amenazas, sino como un instrumento de gestión estructurada, donde su propósito es servir como base para el cumplimiento del Plan de Tratamiento de Riesgos, permitiendo definir protocolos de respuesta, controles técnicos y administrativos, y mecanismos de seguimiento que aseguren la recuperación institucional frente a incidentes de seguridad, donde cada riesgo descrito en la tabla está vinculado con una causa raíz, que identifica el origen técnico u organizacional del problema; una consecuencia, que refleja el impacto directo sobre la operación, la continuidad asistencial y la confianza institucional; y una evaluación de probabilidad e impacto, que determina el nivel de riesgo conforme a la metodología de la matriz. Además, se incluye la referencia normativa al delito informático correspondiente en el Código Penal Colombiano, lo cual aporta trazabilidad legal y fortalece la capacidad de respuesta institucional frente a investigaciones o procesos sancionatorios.

Riesgo	Causa	Consecuencia	Probabilidad	Impacto	Nivel de Riesgo	Delito informático asociado
Pérdida de datos	Falla crítica en servidores o infraestructura tecnológica	Interrupción en la prestación de servicios y afectación a la continuidad asistencial	Alta	Crítico	Crítico	Daño informático (Art. 269D)
Acceso no autorizado	Uso de contraseñas débiles o gestión inadecuada de credenciales	Exposición y divulgación de información sensible, incluyendo datos personales y clínicos	Alta	Alto	Alto	Acceso abusivo a sistema informático (Art. 269A)
Fuga de datos	Filtración por vulnerabilidades en aplicaciones o accesos indebidos	Pérdida de confianza institucional, sanciones legales y afectación a derechos de titulares de datos	Alta	Crítico	Crítico	Violación de datos personales (Art. 269F)
Ataques DDoS	Saturación deliberada de servicios por tráfico malicioso externo	Caída de plataformas digitales, interrupción de servicios misionales y afectación reputacional	Media	Alto	Alto	Obstaculización ilegítima de sistema informático o red (Art. 269E)
Ransomware	Ejecución de malware que cifra información y	Paralización de servicios, pérdida de datos críticos,	Media	Crítico	Crítico	Hurto por medios informáticos (Art.

Riesgo	Causa	Consecuencia	Probabilidad	Impacto	Nivel de Riesgo	Delito informático asociado
	exige pago para liberarla	extorsión financiera y exposición legal				269I) + Extorsión (Art. 244)
Suplantación de identidad	Uso fraudulento de credenciales o perfiles institucionales para acceder a sistemas	Acceso indebido a información confidencial, alteración de registros y afectación a la trazabilidad operativa	Alta	Alto	Alto	Falsedad personal (Art. 296–297) + Acceso abusivo (Art. 269A)
Phishing	Envío de correos electrónicos, mensajes o sitios web falsos que simulan ser legítimos	Robo de credenciales, fraude financiero, acceso indebido a sistemas institucionales y exposición de datos personales	Alta	Crítico	Crítico	Hurto por medios informáticos (Art. 269I) + Estafa (Art. 246)

Tabla No. 1 Tabla de riesgos de seguridad de la información.

Estas actividades, integradas en un ciclo de mejora continua, permiten que la Secretaría Distrital de Salud cuente con un sistema de gestión de riesgos sólido, capaz de anticipar amenazas, reducir vulnerabilidades y garantizar la resiliencia institucional frente a incidentes de seguridad de la información.

8. Actividades de Gestión del Riesgo 2026

El cronograma anual de actividades para la vigencia 2026 constituye un instrumento de planificación estratégica que organiza, distribuye y da seguimiento a las acciones definidas en el Plan de Tratamiento de Riesgos y Seguridad de la Información de la Secretaría Distrital de Salud, se estructura de manera trimestral, garantizando ejecución ordenada, responsables claramente definidos y metas verificables que faciliten la evaluación de resultados.

Cada actividad cuenta con responsables definidos por área, la línea institucional la guiará la Dirección de Planeación Institucional y Calidad, incluyendo el apoyo de la Dirección Tecnologías de la Información y las dependencias misionales estarán participando de las actividades necesarias para cumplir con las metas establecidas en este plan y que son expresadas en indicadores de cumplimiento que permiten verificar el avance del plan y asegurar la mejora continua.

Actividades Principales	Responsables Clave	Trimestre / Meses
- Inventario de activos de información - Revisión inicial de la matriz de riesgos -Capacitación y sensibilización del personal institucional y terceros con acceso a información.	Dirección TIC´s, Dirección de Planeación Institucional y Calidad, Dependencias misionales	Enero – Marzo
- Análisis y evaluación de riesgos. - Aplicación de metodologías de probabilidad/impacto - Definición de controles iniciales	Dirección TIC´s, Dirección Jurídica, Comité de Seguridad de la Información. Dirección de Planeación Institucional y Calidad.	Abril – Junio
- Monitoreo de controles - Revisiones documentales - Pruebas de seguridad sobre sistemas críticos -Capacitación y sensibilización del personal institucional y terceros con acceso a información.	Dirección TIC´s, Dependencias misionales, Dirección de Planeación Institucional y Calidad	Julio – Septiembre
- Capacitación y sensibilización del personal - Consolidación de informes de seguimiento - Presentación de resultados a la alta dirección	Dirección de Planeación Institucional y Calidad Dirección TIC´s, Dirección Jurídica, Alta Dirección, Comité de Seguridad de la Información	Octubre – Diciembre

9. Indicadores de evaluación y seguimiento

El Sistema de Gestión de Riesgos de la Secretaría Distrital de Salud requiere mecanismos objetivos, verificables y auditables que permitan medir el grado de avance y la efectividad de las actividades definidas en este plan, para tal fin, se han establecido indicadores de evaluación y seguimiento, diseñados bajo criterios de pertinencia, claridad, trazabilidad y medible, garantizando que los resultados puedan ser reportados y utilizados como insumo para la mejora continua institucional.

Estos indicadores cumplen tres funciones esenciales:

- Asegurar la trazabilidad de las acciones ejecutadas.
- Verificar el cumplimiento de metas establecidas en el plan.
- Identificar oportunidades de mejora en la gestión de riesgos y seguridad de la información.

9.1. Inventarios de Activos de Información por Área

Este indicador mide el número de inventarios programados a realizar contra los inventarios efectivamente realizados y actualizados en cada dependencia institucional, ya que su importancia radica en que los inventarios constituyen la base para la identificación de riesgos, ya que permiten conocer con precisión qué sistemas, bases de datos y procesos críticos existen y dónde se encuentran, la actualización periódica asegura que los cambios en infraestructura tecnológica, procesos administrativos o incorporación de nuevos sistemas sean reflejados oportunamente, para que de esta manera, se garantice que la gestión de riesgos se realice sobre información confiable y completa, evitando vacíos que puedan comprometer la seguridad institucional.

Indicador: # de inventarios programados por realizar - # de Inventarios realizados / # de inventarios programados por realizar * 100

9.2. Actualización de la Matriz de Riesgos

La matriz de riesgos es el instrumento central para la identificación, valoración y priorización de riesgos, este indicador evalúa la frecuencia y calidad de las actualizaciones realizadas, asegurando que los riesgos emergentes derivados de cambios tecnológicos, normativos o del entorno institucional sean incorporados oportunamente, porque una matriz desactualizada genera un sesgo en la toma de decisiones, mientras que una matriz dinámica y vigente permite a la SDS anticiparse a amenazas y ajustar sus controles de manera proactiva con lo que en este sentido, el indicador no solo mide cumplimiento, sino también la capacidad de adaptación institucional frente a un entorno cambiante.

Indicador: # de actualización de matriz de riesgos programadas - # de matriz de riesgo realizadas / # de actualización de matriz de riesgos programadas * 100

9.3. Controles Monitoreados vs. Controles Seleccionados

Este indicador mide la proporción de controles efectivamente monitoreados frente al total de controles definidos en el plan. Su relevancia es doble, ya que por un lado, asegura que los controles implementados para mitigar riesgos sean revisados de manera sistemática; por otro, permite documentar evidencias y ajustar medidas en caso de detectar debilidades o incumplimientos. La verificación continua fortalece la confianza en el sistema de gestión, ya que demuestra que los controles no son estáticos, sino que se someten a un ciclo de mejora permanente. Además, este indicador facilita la rendición de cuentas, consolidando la transparencia institucional.

Indicador: # de controles efectivamente monitoreados / #
total de controles definidos en el plan * 100

9.4. Capacitaciones Ejecutadas vs. Capacitaciones Planeadas

La construcción de una cultura organizacional de ciberseguridad depende en gran medida de la formación y sensibilización del personal, este indicador mide el número de actividades de capacitación realizadas en comparación con las programadas, reflejando el compromiso institucional con el desarrollo de competencias en seguridad de la información.

Para conservar una curva de aprendizaje y apropiación del conocimiento se llevaran a cabo cuatro campañas de capacitación relacionada con el Sistema de Gestión de la Seguridad de la Información y la Protección de Datos Personales, dando sustento, este indicador que permite evaluar el impacto de las capacitaciones en la preparación del personal para responder ante incidentes y aplicar buenas prácticas en su trabajo diario, lo que en consecuencia, se convierte en un mecanismo para fortalecer la protección institucional y reducir la probabilidad de incidentes derivados de errores humanos o desconocimiento.

Indicador: # de capacitaciones realizadas / # de capacitaciones programadas * 100

9.5. Actualización y Cobertura de la Matriz BIA

Este indicador mide el grado de actualización y cobertura de la **Matriz de Análisis de Impacto al Negocio (BIA)**, evaluando tanto la frecuencia con la que se revisa como la proporción de procesos críticos efectivamente analizados frente al total de procesos institucionales.

La matriz BIA es un instrumento fundamental para identificar las funciones esenciales de la Secretaría Distrital de Salud, determinar los tiempos máximos de recuperación aceptables (RTO) y establecer las dependencias críticas de recursos tecnológicos, humanos y normativos, este indicador asegura que el análisis de impacto se mantenga vigente y alineado con la realidad operativa, considerando cambios en la estructura organizacional, nuevas regulaciones o transformaciones digitales.

Indicador: # de procesos críticos analizados / # total procesos institucionales *100

10. Recursos humanos, técnicos, logísticos y financieros

La implementación efectiva del Plan de Tratamiento de Riesgos y Seguridad de la Información de la Secretaría Distrital de Salud requiere de una adecuada provisión de recursos que aseguren la sostenibilidad y la eficacia de las acciones definidas, donde estos recursos se estructuran en cuatro categorías principales: humanos, técnicos, logísticos y financieros, cada uno de ellos con un papel fundamental en la consolidación de un sistema de gestión robusto.

Componente Humano: El plan contempla la participación del Oficial de Seguridad de la Información, quien lidera la estrategia institucional y asegura la alineación con las normas ISO/IEC 27001 de 2022 y el MSPI, asimismo, los líderes de procesos tienen la

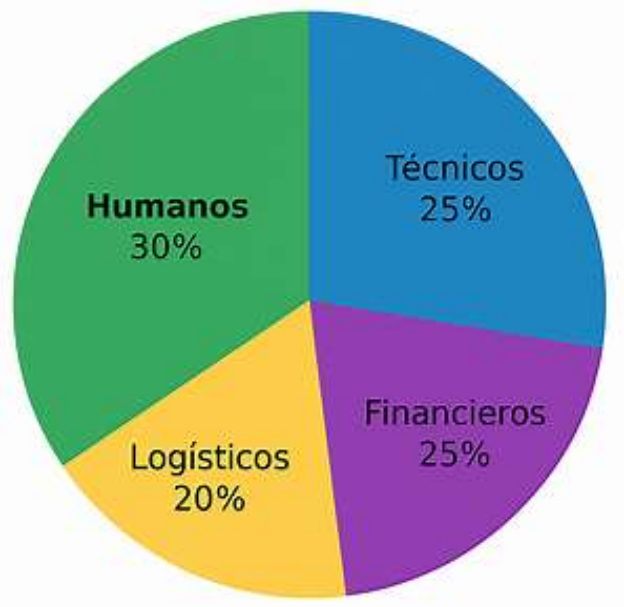
responsabilidad de identificar riesgos específicos en sus áreas, aportar evidencias y garantizar la aplicación de controles.

El equipo de Tecnologías de la Información (TI) constituye un soporte esencial para la implementación de medidas técnicas, la administración de plataformas digitales y la respuesta ante incidentes de seguridad, la articulación de estos actores asegura que la gestión de riesgos se realice de manera transversal y coordinada.

Componente de Recursos Técnicos: Se incluyen las herramientas del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), matrices de riesgos actualizadas y sistemas de monitoreo que permiten identificar vulnerabilidades y evaluar la efectividad de los controles, donde estas herramientas garantizan la trazabilidad documental.

Componente de Recursos logísticos: Están orientados a facilitar la socialización del plan y la capacitación del personal y se contemplan espacios físicos y virtuales para la realización de talleres, jornadas de sensibilización y entrenamientos especializados en seguridad de la información y ciberseguridad, ya que estos recursos aseguran que la cultura organizacional de protección de la información se fortalezca y que todos los funcionarios y contratistas comprendan su rol en la gestión de riesgos.

Componente Financiero: Garantiza la disponibilidad presupuestal para ejecutar las acciones del plan de manera efectiva y sostenible, debe incluir la financiación de herramientas tecnológicas, capacitaciones, consultorías y controles de seguridad, ya que su adecuada planificación permite cumplir cronogramas, demostrar cumplimiento normativo (ISO/IEC 27001, MSPI), además, asegura que el SGSPI cuente con respaldo económico para su operación continua y mejora progresiva.



11. Tratamiento de riesgos

El tratamiento de riesgos constituye la fase estratégica del proceso de gestión de seguridad de la información, en la cual la Secretaría Distrital de Salud define y aplica las medidas necesarias para reducir la probabilidad de ocurrencia y el impacto de los eventos que puedan comprometer la confidencialidad, integridad y disponibilidad de los activos institucionales.

Este proceso se desarrolla bajo los lineamientos de la norma ISO 31000 de 2018 y la ISO/IEC 27001 de 2022, garantizando que cada decisión esté sustentada en criterios técnicos, normativos y de costo-beneficio, y que se mantenga la trazabilidad documental para fines de control.

La primera estrategia corresponde a evitar el riesgo, lo que implica la suspensión o eliminación de actividades que generen una exposición significativa y que no puedan ser controladas de manera efectiva, con este escenario, la entidad opta por no ejecutar procesos que representen amenazas críticas para la seguridad de la información, priorizando la protección de los datos sensibles, para dar paso luego a la continuidad de los servicios esenciales.

La segunda estrategia es mitigar el riesgo, mediante la implementación de controles técnicos, organizativos y legales que reduzcan la probabilidad de ocurrencia o el impacto de los incidentes; entre estos controles se incluyen mecanismos de autenticación robusta, incluyendo doble nivel de autenticación, cifrado de datos, segmentación de redes, políticas de acceso y programas de capacitación, porque la mitigación busca fortalecer la resiliencia institucional y garantizar que los riesgos se mantengan dentro de niveles aceptables.

La tercera estrategia consiste en **transferir el riesgo**, lo que se logra a través de la contratación de seguros especializados en seguridad digital o mediante la tercerización de servicios tecnológicos con proveedores que cuenten con certificaciones y estándares internacionales, lo que permite compartir la responsabilidad y reducir la carga financiera o técnica que implicaría la materialización de ciertos riesgos, asegurando que la entidad mantenga su capacidad operativa frente a eventos adversos.

Finalmente, se contempla la estrategia de aceptar el riesgo, aplicable a aquellos escenarios de bajo impacto o probabilidad, en los cuales el costo de implementar controles adicionales supera el beneficio esperado; la aceptación de riesgos se realiza de manera consciente y documentada, estableciendo mecanismos de seguimiento y monitoreo que permitan verificar que dichos riesgos no evolucionen hacia niveles críticos.

En conjunto, estas cuatro estrategias conforman un marco integral de tratamiento de riesgos que asegura la protección de los activos de información de la Secretaría Distrital de Salud, optimiza el uso de recursos institucionales y fortalece la capacidad, donde Este enfoque permite que la entidad gestione sus riesgos de manera proactiva, equilibrando la seguridad con la eficiencia operativa y la sostenibilidad institucional.

12. Monitoreo y mejora continua

El monitoreo y la mejora continua constituyen pilares fundamentales en la gestión de riesgos de seguridad de la información de la Secretaría Distrital de Salud, asegurando que los controles implementados mantengan su efectividad y que el sistema de gestión se adapte a los cambios tecnológicos, normativos y organizacionales, para que este proceso se desarrolle bajo un enfoque de ciclo de mejora continua, alineado con la metodología de la norma ISO 31000 de 2018, que establece la necesidad de revisar, retroalimentar y optimizar cada etapa de la gestión de riesgos. El segundo componente corresponde a la definición y seguimiento de KPIs (Key Performance Indicators) de efectividad de controles, los cuales permiten medir de manera objetiva el desempeño de las medidas implementadas, para que estos indicadores incluyen métricas como el porcentaje de controles ejecutados frente a los planificados, el tiempo de respuesta ante incidentes, la reducción de vulnerabilidades críticas y el nivel de cumplimiento normativo, ya que el análisis de KPIs facilita la toma de decisiones estratégicas, prioriza recursos y asegura que los esfuerzos de mitigación generen resultados tangibles y verificables.

La tercera actividad clave es la revisión periódica y la trazabilidad documental, que garantizan que los registros de riesgos y controles se mantengan actualizados y disponibles para consulta, la trazabilidad documental permite demostrar la correcta aplicación de la metodología, la efectividad de los controles y la evolución del sistema de gestión en el tiempo, esta práctica asegura que cada acción esté respaldada por evidencia verificable, fortaleciendo la confianza institucional y la capacidad de defensa en escenarios de supervisión. Diagrama de flujo de metodología ISO 31000 incluido en el proceso de monitoreo y mejora continua se representa mediante un diagrama de flujo basado en la metodología ISO 31000, que ilustra las etapas de establecimiento del contexto, identificación, análisis, evaluación, tratamiento, monitoreo y retroacción ya que este recurso gráfico facilita la comprensión del ciclo de gestión de riesgos, mostrando cómo cada fase se interrelaciona para la mejora continua del sistema.

13. Conclusiones y compromiso institucional

El Plan de Tratamiento de Riesgos y Seguridad de la Información de la Secretaría Distrital de Salud se consolida como una herramienta fundamental para la gestión proactiva de riesgos, al integrar metodologías internacionales, lineamientos nacionales y buenas prácticas institucionales en un marco coherente donde su aplicación permite anticipar escenarios de amenaza, reducir vulnerabilidades y garantizar la resiliencia de los procesos misionales, administrativos y tecnológicos, asegurando que la información se mantenga protegida frente a riesgos internos y externos.

La estructuración del plan bajo los estándares ISO/IEC 27001 de 2022 y ISO 31000 de 2018, junto con el Modelo de Seguridad y Privacidad de la Información (MSPI), fortalece la capacidad institucional para enfrentar procesos de certificación.

En este sentido, el documento constituye una base sólida para la preparación de institucional frente a la norma ISO/MSPI previstas para el año 2026, garantizando que cada control, procedimiento y evidencia se encuentre debidamente documentado y trazable, con el fin de la adopción de indicadores de desempeño, cronogramas verificables y registros de controles.

Finalmente, el plan refleja el compromiso institucional firmado por la alta dirección, lo que asegura su legitimidad y sostenibilidad en el tiempo, porque este compromiso se traduce en la asignación de recursos humanos, técnicos, logísticos y financieros, así como en la promoción de una cultura organizacional del cuidado de la información y la ciberseguridad.

La alta dirección reconoce que la protección de la información es un eje transversal para la confianza ciudadana, la transparencia administrativa y la continuidad de las actividades misionales, administrativas y operativas.

En conclusión, el Plan de Tratamiento de Riesgos y Seguridad de la Información no solo responde a las exigencias normativas y técnicas, sino que también reafirma la voluntad institucional de la Secretaría Distrital de Salud de avanzar hacia un modelo de gestión robusto, preventivo y sostenible, capaz de enfrentar los desafíos de la era digital y de garantizar la seguridad de la información en beneficio de la ciudadanía.

14. Definiciones

Término	Definición	Traducción / Significado	Explicación
SDS	Secretaría Distrital de Salud	*Bogotá District Health Secretariat*	Entidad pública responsable de la gestión sanitaria en Bogotá, incluyendo servicios asistenciales, vigilancia epidemiológica y cumplimiento normativo en seguridad de la información.

PSPI	Plan de Seguridad y Privacidad de la Información	*Information Security and Privacy Plan*	Documento institucional que formaliza controles, protocolos y procedimientos para proteger la confidencialidad, integridad y disponibilidad de la información.
SGSI	Sistema de Gestión de Seguridad de la Información	*Information Security Management System (ISMS)*	Conjunto de políticas, procesos y controles que permiten gestionar riesgos de información de forma sistemática, basado en ISO/IEC 27001.
MSPI	Modelo de Seguridad y Privacidad de la Información	*Information Security and Privacy Model*	Marco metodológico del MinTIC que articula la política pública de seguridad digital con prácticas institucionales de gestión de riesgos.
ISO/IEC 27001	Norma internacional de seguridad de la información	*ISO/IEC 27001 Standard*	Estándar que define requisitos para implementar y mantener un SGSI, asegurando protección frente a amenazas internas y externas.
ISO 31000	Norma internacional de gestión de riesgos	*ISO 31000 Risk Management Standard*	Proporciona principios y directrices para la gestión integral de riesgos, aplicable a cualquier organización.
MIPG	Modelo Integrado de Planeación y Gestión	*Integrated Planning and Management Model*	Marco de referencia para la gestión pública en Colombia, que articula planeación estratégica, gestión del desempeño y mejora continua.
MinTIC	Ministerio de Tecnologías de la Información y las Comunicaciones	*Ministry of Information and Communication Technologies*	Entidad nacional que lidera la política pública de seguridad digital, protección de datos y transformación tecnológica.
CONPES	Consejo Nacional de Política Económica y Social	*National Council for Economic and Social Policy*	Documento técnico que define políticas públicas estratégicas. Ej.: CONPES 3854 (Seguridad Digital) y CONPES 3995 (Ciberseguridad).
Ley 1581 de 2012	Ley de protección de datos personales	*Personal Data Protection Law*	Regula el tratamiento de datos personales en Colombia, estableciendo principios de legalidad, finalidad, libertad y seguridad.
Decreto 1377 de 2013	Reglamenta la Ley 1581	*Decree 1377 of 2013*	Define procedimientos para autorización y manejo de datos sensibles.
Decreto 1078 de 2015	Decreto Único Reglamentario del sector TIC	*Single Regulatory Decree for ICT Sector*	Consolida disposiciones sobre seguridad digital y gestión de información en entidades públicas.

Resolución 500 de 2021	Lineamientos de seguridad digital del MinTIC	*Resolution 500 of 2021*	Adopta lineamientos específicos para la estrategia de seguridad digital en entidades públicas.
WAF	Web Application Firewall	*Firewall de Aplicaciones Web*	Filtra y bloquea tráfico HTTP/HTTPS hacia aplicaciones web, protegiendo contra ataques como SQL Injection y XSS.
DDoS	Distributed Denial of Service	*Denegación de Servicio Distribuida*	Ataque que busca saturar recursos de un sistema mediante múltiples solicitudes simultáneas, afectando disponibilidad.
VPN	Virtual Private Network	*Red Privada Virtual*	Conexión cifrada que garantiza confidencialidad en la comunicación entre sistemas on-premise y recursos en la nube.
On-premise	Infraestructura tecnológica local	*On-premise Infrastructure*	Sistemas y servidores instalados físicamente en la entidad, en contraste con servicios en la nube.
Phishing	Técnica de fraude digital	*Phishing Attack*	Estrategia de ingeniería social para engañar usuarios y obtener credenciales o datos sensibles mediante correos o sitios falsos.
Ransomware	Malware de secuestro de información	*Ransomware*	Software malicioso que cifra datos y exige pago para liberarlos, afectando disponibilidad y generando extorsión.
Mapa de calor	Herramienta de visualización de riesgos	*Risk Heat Map*	Representación gráfica que muestra la criticidad de riesgos según probabilidad e impacto.
Ficha Técnica de Riesgo	Documento de detalle de riesgos	*Risk Technical Sheet*	

15. Control de cambios.

VERSIÓN	FECHA DE APROBACIÓN	RAZÓN DE ACTUALIZACIÓN
1	Enero de 2026	Se define el Plan de Tratamiento de Riesgos de Seguridad de la información para la vigencia 2026.