PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES.

2026

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

Contenido

1. OBJETIVO:

La Secretaría Distrital de Salud (SDS) gestiona información crítica para la salud pública, por lo que este plan tiene como objetivo desarrollar un Sistema de Gestión de Seguridad de la Información que garantice la protección de dicha información, minimizando riesgos, asegurando cumplimiento normativo y que permita establecer el marco general del SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, alineado con la misión institucional de la SDS y los requisitos normativos.

Este Plan de seguridad y privacidad de la información busca la transformación digital institucional, la expansión de servicios en la nube y la intensificación del tratamiento de datos personales, busca tener estrategias y herramientas que disminuyan las amenazas cibernéticas que han elevado el numero incidentes de manera significativa los riesgos asociados a la Confidencialidad, Integridad y Disponibilidad (CID) de la información. En este contexto, la Entidad ha venido implantando acciones de seguridad de la información desde planes previos, las cuales requieren consolidación, madurez y alineación normativa conforme a los lineamientos actualizados del Modelo de Seguridad y Privacidad de la Información (MSPI) y las normas ISO/IEC 27001 de 2022.

Este Plan de Seguridad y Privacidad de la Información constituye el instrumento rector para el gobierno de la seguridad de la información, garantizando la alineación entre la estrategia institucional, el Modelo Integrado de Planeación y Gestión (MIPG), la Política de Gobierno Digital, y las mejores prácticas internacionales en gestión de riesgos de información.

Por lo tanto, la Dirección de Planeación Institucional y Calidad desarrollará este Plan, que adopta un enfoque preventivo, basado en riesgos y orientado a resiliencia digital, protección de la información, protección de la infraestructura Tecnológica incluyendo sus dispositivos y permitiendo a la entidad, anticipar, resistir, responder, documentar y recuperarse frente a incidentes de seguridad y eventos que afecten el tratamiento de la información y los datos personales.

La Secretaría institucionalizará un modelo de aprendizaje continuo basado en la mejora de controles, políticas y estrategias, alineándolo con los requisitos de la norma ISO/IEC 27001 de 2022, a través de la metodología de prevención y uso de controles y lecciones aprendidas previo y tras la ocurrencia de incidentes; el personal participará en análisis prácticos para identificar brechas de seguridad y fallos en la protección de datos.

Este plan utilizará el ciclo de mejora continua (PHVA) que permitirá establecer, implementar, mantener y mejorar de manera continua el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) de la Entidad, mediante la definición de controles, estrategias, responsabilidades, mecanismos de seguimiento y evidencias, orientados a la protección integral de la información y los datos personales, garantizando su Confidencialidad, Integridad y Disponibilidad.

Para esto se utilizarán los siguientes componentes:

- Fortalecer el gobierno institucional de la seguridad de la información.
- Asegurar la alineación del SGSPI con los objetivos misionales y estratégicos.
- Incrementar la resiliencia digital frente a amenazas internas y externas.
- Integrar la privacidad por diseño y por defecto en todos los procesos.
- Documentar, capacitar, socializar y analizar incidentes de Seguridad de la Información.
- Incentivar la Cultura Institucional para el cuidado de la información y para aumentar los controles, en el día a día y en los puestos de trabajo.

La Secretaría ha definido de manera clara los lineamientos, procedimientos y estándares de seguridad para la protección de la información y datos personales a través de la Política General de Seguridad de la Información de la Secretaría Distrital de Salud Resolución 705 del 11 de julio de 2025 que esta alineada con la norma ISO/IEC 27001 de 2022, por lo que este marco documental no solo servirá como guía para el cumplimiento, sino que normalizará las conductas institucionales para garantizar que cada proceso técnico, asistencial y administrativo cuente con lineamientos precisos que protejan la confidencialidad, integridad y disponibilidad de los datos en general de la Secretaría.

Se establece este plan con el propósito de proteger los activos de información (datos, procesos, hardware, software) de la organización mediante directrices claras para reducir los riesgos a través de la aplicación de controles de seguridad, blindando la confidencialidad, integridad y disponibilidad de la información, conforme a los requisitos legales y organizacionales.

1.1. OBJETIVOS ESPECÍFICOS:

1. Facilitar la evaluación de la madurez del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), por medio de registros trazables y verificables que permiten reconstruir la historia de cualquier tratamiento de datos o respuesta ante incidentes.
2. Identificar, analizar, y tratar los riesgos de seguridad de la información, considerando activos, procesos, tecnologías y terceros, tomando criterios de

impacto y probabilidad sobre la Confidencialidad Integridad Disponibilidad (CID).

3. Implementar controles técnicos, organizacionales y legales alineados con ISO/IEC 27001 de 2022 y 27701, asegurando su coherencia con el MSPI.
4. Garantizar la seguridad de la información y el tratamiento ético de la información y los datos personales durante todo su ciclo de vida, integrando principios de privacidad, transparencia y responsabilidad, conforme a los estándares internacionales.
5. Fortalecer las capacidades institucionales de aprendizaje, detección, respuesta y recuperación ante incidentes de seguridad.
6. Establecer mecanismos de control, seguimiento, medición y mejora continua, soportados en indicadores y evidencias.

La Entidad cuenta con controles parciales implementados, con niveles de madurez heterogéneos y brechas identificadas en monitoreo continuo, seguridad en la nube y gestión avanzada de identidades.
Al finalizar la vigencia 2026, se espera alcanzar un nivel de madurez gestionado y medible, con controles integrados, monitoreo continuo y evidencia suficiente para auditoría externa.

AÑO 2025 (Finalizado)

ESTADO: Base establecida y Diagnóstico inicial completo.

AÑO 2026 (Meta Proyectada)

ESTADO: Maduración, Automatización y Cultura Integral. 100% con una tolerancia del -+10%

2. ALCANCE:

La creciente adopción de entornos digitales donde conviven, convergen y se integran dos mundos, como la infraestructura física tradicional tecnológica y los servicios de acceso y almacenamiento remoto a través de servicios de internet en la nube, sumado a la consolidación del trabajo remoto y la tercerización, exige que la Secretaría Distrital de Salud (SDS) defina un alcance transversal para establecer un Sistema de Gestión de Seguridad de la Información y Protección de Datos Personales interdependiente que elimine brechas de seguridad y garantice que ningún activo de información sin importar si reside en servidores propios o externos, plataformas externas o dispositivos móviles, quede excluido de los mecanismos de protección institucional, así como activos de bienes, planta, dispositivos o equipos,

que por su composición tecnológica se establezcan como prioridad de atención en seguridad.
En consecuencia, el presente Plan establece un marco de cumplimiento y observancia para los siguientes dominios institucionales:

1. Procesal: Aplica a la totalidad de los procesos del mapa institucional, incluyendo los niveles estratégicos, misionales, de apoyo y de evaluación, lo que garantiza que la seguridad de la información esté incluida en la cadena de valor, desde la alta dirección hasta las dependencias estratégicas, administrativas y operacionales.
2. Dominio de Activos de Información: Comprende toda la información generada, procesada o custodiada por la entidad, sin distinción de su formato o soporte (físico, digital, electrónico, auditivo o visual), que incluye datos sensibles y protegidos bajo principios de confidencialidad y reserva legal.

   Un componente crítico de este dominio es la adopción de servicios en la nube, los cuales se gestionan bajo tres modelos fundamentales:

   a. la Infraestructura como Servicio (IaaS), que proporciona los recursos de computación y servidores virtuales.
   b. la Plataforma como Servicio (PaaS), que ofrece entornos optimizados para el desarrollo y despliegue de aplicaciones institucionales;
   c. el Software como Servicio (SaaS), que abarca las aplicaciones listas para el uso final, como el correo electrónico o herramientas de colaboración.

3. Dominio del Talento Humano y Tercerización: Su cumplimiento es obligatorio para la totalidad de los servidores públicos, contratistas, pasantes y colaboradores, asimismo, se extiende a terceros y proveedores de servicios, quienes deberán alinearse contractualmente a los estándares de seguridad y privacidad definidos por la SDS.
4. Dominio Tecnológico e Infraestructura: Comprende los activos que soportan la operación digital de la Secretaría, Incluye desde la infraestructura física y bases de datos hasta los dispositivos finales utilizados por el personal.

La gestión de estos servicios en la nube implica un modelo de responsabilidad compartida donde la SDS garantiza la seguridad de la información procesada, mientras se supervisan los controles de los proveedores externos y sin excluir este dominio se extiende a las infraestructuras críticas y a todos los canales de comunicación oficiales dado que el objetivo es asegurar que el tratamiento de datos personales y la prestación de servicios digitales se realicen bajo un esquema de

protección unificado, eliminando puntos ciegos en la custodia y administración de la información sin importar el modelo tecnológico empleado.

3. MARCO NORMATIVO

La gestión de la seguridad y privacidad de la información en la Secretaría Distrital de Salud (SDS) se fundamenta en una articulación coherente entre estándares internacionales, marcos nacionales obligatorios y políticas de transformación digital, por lo que este Plan adopta un enfoque integrador que trasciende la simple citación normativa, buscando la Implementación y despliegue técnico de cada requisito dentro del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSI), generando con rigor el objetivo primordial que es convertir las obligaciones normativas y legales en controles organizacionales efectivos, garantizando una trazabilidad total que facilite la demostración de cumplimiento ante entes de control y elimine la dispersión documental histórica.

3.1. Estándares Internacionales de Referencia (ISO/IEC):

Es el pilar estructural del sistema es la norma ISO/IEC 27001 de 2022, la cual proporciona la metodología para una gestión sistemática de riesgos en que su desarrollo impacta al SGSI mediante la identificación rigurosa de activos, dispositivos, amenazas, riesgos y vulnerabilidades, introduciendo controles que incluyen la modernización para entornos físicos locales y de acceso remoto en la nube.

Por su parte, la ISO/IEC 27701 actúa como una extensión crítica dedicada a la privacidad, obligando a la entidad a gestionar el ciclo de vida de los datos personales bajo los roles responsables o encargados del Tratamiento, llevando a que en la ejecución de evaluaciones del SGSI y la consolidación de inventarios de datos con sus respectivos registros de consentimiento y atención a derechos del titular, sea parte operacional.

3.2. Marcos Nacionales y Políticas Públicas (MSPI, MIPG y Gobierno Digital)

A nivel nacional, el Plan se alinea estrictamente con el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y las Resoluciones 500 de 2021 y 2277 de 2025, que imponen el ciclo PHVA como motor de mejora continua donde esta estructura se une con el Modelo Integrado de Planeación y Gestión (MIPG) del Departamento Administrativo de la Función Pública (DAFP), permitiendo que la seguridad de la información y protección de datos personales deje de ser un proceso aislado para convertirse en un componente del control que apoya los objetivos institucionales, también bajo la Política de Gobierno Digital del Ministerio de Tecnologías de la

Información y las Comunicaciones (MinTIC) a través del Decreto 1151 de 2008 de Gobierno en Línea y en el Decreto 1008 de 2018 Política de Gobierno Digital, el Decreto 1078 de 2015 con el que se consolidó la seguridad de la información incluyendo los datos personales como una política de Estado en el sector TIC, adicional el Decreto 767 de 2022 que actualiza Decreto Único Reglamentario 1078, para que las estrategias y planes de seguridad de la información sea posicionado como el habilitador fundamental de los servicios ciudadanos, garantizando la confianza digital y la protección de los datos en todos los procesos de interoperabilidad de las entidades Públicas.

Actualmente, la Entidad reconoce un estado de cumplimiento parcial caracterizado por evidencias fragmentadas y una necesidad latente de integración documental, la proyección para el periodo 2026 se orienta hacia la consolidación de un sistema de cumplimiento trazable, verificable y totalmente alineado entre los estándares ISO, el MSPI y el MIPG, para el que se busca la mejora continua, el aprendizaje y la aplicación de estrategias para protección de datos personales y la información que desde la gestión de hallazgos conduzca a la madurez de los sistemas asociados a cada política y procedimiento aprobado y que genere evidencias contundentes de una cultura de seguridad institucional fortalecida y madura.

Gráfica No. 1 Jerarquía normativa.

4. DOCUMENTOS DE REFERENCIA

El cuerpo documental de referencia constituye el andamiaje técnico y normativo esencial para el despliegue del presente Plan ya que su articulación no solo asegura la trazabilidad histórica de las acciones de seguridad, sino que también maximiza la eficiencia operativa al mitigar la duplicidad de esfuerzos, proyectando un nivel de madurez institucional sólido ante organismos de control internos y externos.

Este marco de gobernanza integra de forma armónica los conceptos del Reglamento General de Protección de Datos de la Ley 1581 de 2012, alineándose estrictamente

con el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio TIC de Colombia, al converger con las políticas internas y directrices técnicas, este Plan define con precisión el alcance, las responsabilidades y las salvaguardas críticas necesarias para blindar la integridad, disponibilidad y confidencialidad de los activos de información.

4.1. Insumos y Documentos Fuente

El presente Plan se fundamenta en la integración técnica y armónica de los siguientes instrumentos, garantizando la interoperabilidad normativa y la continuidad de la estrategia institucional:

- Trazabilidad Estratégica: Consolida los aprendizajes y controles establecidos en los Planes de Seguridad y Privacidad de la Información de la vigencia 2025 y 2026.
- Resolución 705 de 2025: Documento Maestro el cual actúa como la directriz principal de la planeación estratégica de Seguridad de la Información y protección de datos personales.
- Manual de la política de Seguridad de la Información: Incorpora el marco vigente de estrategias de seguridad tratamiento de datos personales, asegurando el cumplimiento procedimental, controles y normatividad vigente.
- Cultura, Resiliencia y Capacidad Operativa: Integra los protocolos de Tecnologías de la Información, el Lineamientos Generales de Recuperación ante Desastres Tecnológicos (DRP), los documentos asociados a la Mesa técnica de Incidente, los documentos asociados a la Mesa Técnica de Cambio, junto con sus Gestores, los Planes de Continuidad del Negocio, el Análisis de Impacto al Negocio (BIA) y los esquemas de respuesta, documentos y acciones documentadas ante incidentes de información y de ciberseguridad para una gestión de crisis efectiva.

4.2. Jerarquía Normativa y Criterios de Prevalencia

Con el propósito de mitigar riesgos jurídicos y técnicos ante posibles discrepancias en la interpretación documental, se establecen los siguientes criterios de prelación:
Criterio de Cronología (Lex Posterior): Ante disposiciones contrapuestas, tendrá prevalencia la norma o documento de actualización más reciente, reconociendo la evolución dinámica de las amenazas digitales.

Criterio de Especialidad y Rigor Técnico: Prevalecerá el estándar que ofrezca el nivel más alto de protección de activos, priorizando la alineación con estándares

internacionales como la Norma ISO/IEC 27001 de 2022 y los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI).

4.3. Diagnóstico Estratégico y Hoja de Ruta de Mejora

Si bien la Secretaría cuenta con una base documental robusta, se identifica una fragmentación operativa que limita la cohesión de la información y que como consecuencia, la visión estratégica para el presente periodo se orienta a la transición hacia el establecimiento de estrategias para que de manera concreta se establezca un Sistema de Seguridad de la Información acorde con las necesidades de la Secretaría y que sea alineado con la normatividad.

Con el fin de utilizar el modelo PHVA se creará la Mesa Técnica de Incidentes, y se fortalecerá la Mesa Técnica de Cambios, que evaluaran las estrategias pertinentes para proteger la información.

5. ESTADO ACTUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El estado actual del SGSPI evidencia un nivel de madurez intermedio ejecutado al 54%, con fortalezas en definición de políticas, pero brechas en monitoreo continuo, seguimiento automatización y gestión avanzada de riesgos, por esto el Plan 2025 ya había identificado la necesidad de cerrar brechas críticas en temas como Criptografía, activos de información, tratamiento de riesgos y Gestión de Incidentes, que reportan desarrollo mesurados.

Aspectos evaluados:

Gobierno y Organización: Los roles y responsabilidades están definidos en la documentación inicial, No obstante, existen oportunidades de mejora en la segregación de funciones.

Gestión de Riesgos: La SDS cuenta con una matriz de riesgos existente y planifica actividades de identificación y valoración de riesgos. La oportunidad de mejora se establece en que existe un análisis reciente sobre el Análisis de Impacto al Negocio (BIA), que se crea hacia el cuarto trimestre del año 2025 lo que genera riesgos residuales no identificados ni documentados, pero da oportunidad clara de mejoras y atención a las brechas de seguridad.

Controles Técnicos: La implementación es parcial, Se evidencia la necesidad de fortalecer la seguridad en entornos cloud, remotos, limitar el acceso a redes sociales y paginas web que ofrecen alternativas de solución y edición para documentos

imágenes y videos y la adopción de estrategias de uso relacionado con la Inteligencia Artificial, así como la adopción de controles adecuados y actualizados.

Privacidad: Existe un cumplimiento normativo básico basado en la Ley 1581 de 2012 y decretos asociados, pero se requiere una mayor integración con los procesos operativos para asegurar el control de acceso a los datos personales, tal como lo exige el Anexo A de la norma ISO27001 de 2022.

Debilidades en la Gestión de Identidades y Accesos: Actualmente, la Secretaría presenta vulnerabilidades operativas debido a la falta de un despliegue integral de la Autenticación Multifactor (MFA) en todos los sistemas críticos y servicios cloud que se requieran, ya que la ausencia parcial de mecanismos de validación de identidad robustos incrementa la superficie de ataque y dificulta el cumplimiento de estándares internacionales de ciberseguridad.

Dependencia de terceros tecnológicos: Existe una dependencia crítica de terceros tecnológicos cuya gestión actual es insuficiente; debido a que el plan anterior aborda la relación con proveedores de manera genérica, careciendo de controles específicos, acuerdos de niveles de servicio de seguridad y mecanismos de auditoría. Esta falta de profundidad técnica en la supervisión de proveedores y que carecen de acuerdos actualizados de confidencialidad, genera un riesgo latente de seguridad que podría comprometer la continuidad del negocio y la integridad de los datos.

Exposición en entornos Cloud: La creciente migración de servicios hacia entornos de nube pública, privada e híbrida representa un riesgo crítico si no se cuenta con un marco de gobernanza específico, porque la seguridad en la nube para la Secretaría Distrital de Salud no se limitará a la configuración técnica, sino que requerirá una metodología institucional robusta que garantice el cumplimiento del Esquema Nacional de Seguridad y los lineamientos de Gobierno Digital.

La ausencia de mecanismos documentados de control de acceso, cifrado de datos y monitoreo continuo abre vulnerabilidades que compromete la confidencialidad, privacidad, seguridad y la disponibilidad de los servicios asistenciales de la secretaría.

El presente Plan consolida y eleva el nivel de aspiración de madurez, pasando de controles reactivos a un enfoque preventivo y proactivo para lo que la implementación de una mesa técnica de incidentes y un Centro de Operaciones de Seguridad (SOC) permitirá la detección y respuesta en tiempo real a amenazas que es fundamental para modernizar la arquitectura de seguridad y gestionar accesos remotos y en teletrabajo.

6. ESTRATEGIAS

La seguridad de la información es un pilar estratégico para la Secretaría Distrital de Salud de Bogotá, no un conjunto de controles aislados, donde la evolución constante del panorama de amenazas, que incluye ataques persistentes avanzados, la explotación de credenciales, la fuga de información y los riesgos inherentes a la tercerización tecnológica, exige una estrategia institucional integral por lo que dicho enfoque se alinea con los objetivos misionales, la política de Gobierno Digital y la protección de los datos personales de los ciudadanos.

Este Plan de Seguridad y Privacidad de la Información (PSPI) se basa en el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC, adoptando los controles definidos en el Anexo A de la norma NTC ISO/IEC 27001 de 2022 por que las estrategias responden a un enfoque basado en la gestión de riesgos, priorizando aquellos escenarios que afectan de manera crítica la Confidencialidad, Integridad y Disponibilidad de la información, así como la privacidad de los datos personales y el cumplimiento normativo.

Es imperativo consolidar una gestión de accesos que garantice que solo usuarios autorizados, con vínculos contractuales vigentes tenga acceso a información y operen en la nube, en equipos tecnológicos y dispositivos, lo que estará mitigando así posibles intrusiones derivadas de la gestión ineficaz de contraseñas y protección de estas.

Se establecerá las estrategias para la identificación de accesos como la autenticación, con factores adicionales en transferencias y recibo de información, también incluir el desarrollo de estrategias y actividades para la implantación de controles para fortalecer la seguridad de la información, para que sean identificados por la Declaración de Aplicabilidad (SoA) de la norma ISO27001 del 2022 en su anexo A.

A través de este plan se van a establecer estrategias para que el cifrado incluya más factores y herramientas, para proteger la información y los datos sensibles.

Las estrategias de seguridad y privacidad de la información se formulan bajo los siguientes principios:

- Gestión basada en riesgos.
- Privacidad por diseño y por defecto.
- Automatización y monitoreo continuo.
- Corresponsabilidad institucional.
- Mejora continua bajo el ciclo PHVA.

Cada estrategia articula:

- Riesgos institucionales.
- Controles normativos (ISO/MSPI).
- Tecnologías habilitadoras.
- Evidencias auditables.
- Responsables claramente identificados, sus tareas y responsabilidades.

6.1. Descripción de las Estrategias

Con el propósito de garantizar una gestión integral de la seguridad y privacidad de la información, la Secretaría Distrital de Salud (SDS) ha consolidado un marco estratégico robusto, en el que estas directrices se encuentran alineadas con el Modelo de Seguridad y Privacidad de la Información (MSPI), los lineamientos de la Resolución 500 de 2021 y los estándares internacionales definidos por la norma NTC ISO/IEC 27001.

Cada una de las estrategias diseñadas aborda actividades fundamentales para la protección de la información y datos personales, orientándose específicamente a la mitigación proactiva de riesgos, el fortalecimiento de la resiliencia institucional y la salvaguarda de la continuidad en la prestación de los servicios.

Para alcanzar estos objetivos, la hoja de ruta institucional integra pilares clave como el liderazgo estratégico en seguridad, la gestión técnica de riesgos, el despliegue de controles especializados, la gestión de incidentes y la concientización, para que, asimismo, se priorice la cultura organizacional a través de programas de concienciación y capacitación continua, complementados con protocolos rigurosos para la gestión de incidentes, asegurando así un entorno de información confiable y seguro.

Gráfica No. 2 Pilares Fundamentales del Plan.

Pilar Liderazgo Estratégico de Seguridad de la Información

6.1.1. Estrategia de Protección de Datos Personales

La protección de datos personales constituye un eje estratégico para garantizar el cumplimiento documental y legal y consolidar la confianza ciudadana en la gestión institucional, por eso desde la dirección estratégica en conjunto con la dirección asistencial, se asegurará que todo sistema, proceso y servicio tenga incluido e incorpore controles de seguridad y privacidad desde su concepción.

Se implementarán Evaluaciones de Impacto en la Protección de Datos como mecanismo preventivo para identificar riesgos y definir medidas de mitigación, junto con procesos efectivos para la gestión de los derechos de los titulares, garantizando transparencia, trazabilidad y cumplimiento por la normativa vigente.

En línea con la ISO/IEC 27001 de 2022, se fortalecerán los controles relacionados con la gestión de información personal, incluyendo la clasificación de datos, el control de accesos, la protección en tránsito y reposo, y la auditoría continua de procesos. Asimismo, se adoptarán las directrices del MSPI, asegurando la alineación con los estándares nacionales de seguridad y privacidad aplicables.

6.1.2. Estrategia de Arquitectura Confianza Cero

Los modelos tradicionales de seguridad perimetral han demostrado ser insuficientes frente a los entornos distribuidos actuales, caracterizados por el acceso remoto, la adopción de servicios en la nube y la alta movilidad institucional, por lo tanto, la estrategia de Arquitectura confianza Cero o Zero Trust aborda estas deficiencias.
Este modelo se basa en el principio fundamental de "nunca confiar, siempre verificar", eliminando la confianza implícita que anteriormente se otorgaba a las redes internas, a los controles de acceso basados únicamente en la ubicación física, adicionando controles y políticas que cobran relevancia para proteger el almacenamiento y la entrega de información.

En su lugar, establece un marco de seguridad dinámico centrado en la identidad, el contexto y la mitigación del riesgo.

La implementación de Confianza Cero se sustenta en los siguientes pilares técnicos y de gestión:

Principio	Descripción
Verificación Continua	Autenticación y autorización rigurosa de cada usuario y dispositivo antes de conceder acceso a cualquier recurso.
Acceso de Mínimo Privilegio	Otorgamiento de los permisos estrictamente necesarios para cumplir una función específica, limitando el acceso a información y datos sensibles e importantes, para evitar una brecha en la seguridad.
Microsegmentación Lógica	División de la red en segmentos pequeños y aislados para contener las amenazas y aplicar controles de seguridad granulares.
Evaluación Contextual	Consideración de múltiples factores como: Identificación de Activos, Identificación de ubicación, estado, responsable y características de equipos tecnológicos y dispositivos, ubicación geográfica, identificación del responsable, comportamiento del usuario, con el fin de determinar el nivel de riesgo de un acceso en tiempo real.

Pilar Gestión de Riesgos

6.1.3. Identificación de activos informáticos y tecnológicos.

La SDS cuenta con la identificación de activos de información parcialmente definida y establecerá un proceso institucional para la identificación y gestión de activos informáticos y tecnológicos, garantizando que cada recurso físico, lógico o de información esté registrado en un inventario, con responsable asignado y clasificación según su criticidad.

La estrategia se desarrollará en la definición de roles, levantamiento de información en todas las áreas para identificar activos físicos, lógicos, incluyendo los que encuentran en los servicios Cloud nube, para proceder a clasificarlos por cada activo en el nivel de impacto y que riesgo tiene asociado a su uso en la Secretaría.

Pilar Implementación de controles

6.1.4. Estrategia de Gestión de Identidades y Accesos.

Los accesos no autorizados es uno de los mayores riesgos de seguridad, La Secretaría Distrital de Salud (SDS) establecerá controles sobre quién puede tener accesos a sus datos, información y sistemas; por esto el diagnóstico del Plan de Seguridad de la Información de 2025 obtuvo una calificación de cumplimiento cercana al 54%, que muestra que se necesita mejorar urgentemente la identificación de roles, necesidades, responsabilidades y la Cultura que da forma en la manera en la que manejamos las cuentas de usuario, sus permisos, accesos y la vigencia de estos.

Se buscará revisar la efectividad que tienen los controles para administrar todas las cuentas de usuarios de la entidad, con el objetivo principal de asegurarse de que solo las personas correctas tengan acceso, en el momento correcto, en el tiempo correcto, por el tiempo correcto a la información correcta, sin poner en riesgo los accesos a información y datos.

6.1.5. Estrategia de Criptografía y Protección de la Información

La criptografía es un elemento esencial para proteger la información institucional frente a accesos no autorizados, garantizando la confidencialidad, integridad y trazabilidad de los datos. Actualmente, los mecanismos de cifrado parcial en bases de datos y la gestión manual de claves ofrecen protección básica, pero presentan limitaciones en escalabilidad y control centralizado.

La estrategia para el año 2026 establece la adopción de ser necesario de cifrado robusto, en tránsito (mientras se está transmitiendo) y reposo (información almacenada en bases de datos, discos duros, servidores o respaldos), junto con una gestión centralizada de claves que permita controlar, rotar y auditar su uso desde una plataforma segura, para ello se incorporarán tecnologías avanzadas como módulos de seguridad hardware (HSM), servicios de gestión de claves (KMS) y protocolos de cifrados modernos como TLS, fortaleciendo la seguridad de las comunicaciones y el resguardo de datos críticos.

6.1.6. Estrategia de Prevención de Pérdida de Datos

La prevención de fugas de información sensible es un componente esencial para garantizar la protección de los datos institucionales, porque actualmente, los controles aplicados son principalmente manuales, lo que limita la eficacia y la capacidad de respuesta frente a incidentes.

La estrategia definida para el año 2026 establece la clasificación sistemática de la información según su nivel de sensibilidad y la implementación de soluciones DLP en endpoints, directamente en los dispositivos finales, correo electrónico y servicios en la nube de los usuarios, asegurando un control integral sobre el flujo de datos y reduciendo el riesgo de exposición no autorizada.

6.1.7. Estrategia de Seguridad en la Nube

El creciente uso de servicios SaaS y Cloud computing en la entidad exige fortalecer los controles de seguridad sobre estos entornos, la estrategia para 2026 contempla la implementación de herramientas para la Gestión de la Postura de Seguridad en la Nube como herramienta central para supervisar y asegurar la correcta configuración de los servicios en la nube.

Esta postura permitirá una evaluación continua de configuraciones, garantizando que los recursos Cloud Computing cumplan con las políticas institucionales y normativas aplicables, reduciendo riesgos de exposición y asegurando la protección integral de la información crítica.

6.1.8. Estrategia de Restricción de accesos a redes, aplicaciones y Web

Esta estrategia tiene como objetivo proteger la integridad y confidencialidad de la información institucional mediante el control del uso de enlaces, plataformas y aplicaciones externas que puedan representar riesgos de seguridad, por lo que se implementarán políticas y mecanismos técnicos para limitar el acceso a redes sociales, páginas web y aplicaciones no autorizadas, así como para prevenir el uso de software con vulnerabilidades o posibles puertas traseras.

Esta estrategia se soporta en controles como firewalls, filtrado de contenido, listas blancas y negras de aplicaciones, sistemas que detectan y dan aviso IDS y sistemas que previenen y bloquean IPS y para filtrar el Secure Web Gateway (SWG) que inspeccionará el tráfico de Internet para bloquear amenazas, que permiten bloquear accesos indebidos y monitorear el tráfico en tiempo real.

También en cumplimiento con la ISO/IEC 27001 de 2022, se aplicarán los controles del Anexo A relacionados con el acceso a la información (A.5.19), el control de aplicaciones (A.5.20), y el monitoreo de actividades (A.8.16), asimismo, se garantizará la alineación con el Modelo de Seguridad y Privacidad de la Información MSPI, fortaleciendo la protección de datos personales y sensibles y que como parte de la mejora continua, se realizarán auditorías periódicas, revisiones de políticas de acceso, simulaciones de incidentes y programas de capacitación, asegurando que los controles evolucionen frente a nuevas amenazas y requisitos regulatorios.

Pilar Concientización

6.1.9. Simulacros

Los simulacros de auditoría de incidentes de seguridad de la información, se realizaran para efectos de resiliencia en la seguridad de la información y el proceso de certificación en la norma ISO/IEC27001 de 2022, mínimo una vez al año y tienen como propósito validar el nivel de preparación institucional frente a exigencias normativas, operativas y de respuesta ante eventos críticos de seguridad y ciberseguridad, ya que estos ejercicios permiten identificar brechas, fortalecer la coordinación entre áreas, probar la eficacia de los controles implementados y generar planes de mejora continua, además, garantizan que la seguridad de la información sea auditable, medible, trazable y sostenible, cuando esta alineada con

los controles de la norma ISO/IEC 27001 de 2022 y el Modelo de Seguridad y Privacidad de la Información (MSPI).

6.1.9.1 Simulacro de auditoría ISO/IEC 27001:2022

Para el ejercicio de este Plan se realizarán simulacros de auditoría interna, que buscan replicar las condiciones de una auditoría formal, evaluando la conformidad del SGSI frente a los requisitos de la norma ISO/IEC 27001 de 2022. Se inicia con un Plan de Auditorias que define el alcance, los procesos a evaluar, los criterios de evaluación y el equipo auditor, para que posteriormente se realiza una revisión documental exhaustiva que incluye políticas, procedimientos, matriz de riesgos, declaración de aplicabilidad (SoA), evidencias de seguimiento y mediciones.

Durante la ejecución, se llevan a cabo entrevistas con responsables de procesos, revisión de evidencias operativas (logs, respaldos, tickets, reportes) y observaciones técnicas en campo, los hallazgos se clasifican según su impacto en la confidencialidad, integridad y disponibilidad de la información, y se consolidan en un informe ejecutivo con acciones correctivas, responsables y fechas de cierre, lo que lleva Finalmente a que se actualice el SGSI con base en las lecciones aprendidas, fortaleciendo la trazabilidad y el cumplimiento normativo.

6.1.9.2 Simulacro de incidentes de seguridad de la información

Este simulacro tiene como objetivo evaluar la capacidad institucional para tomar acción y detectar, contener, erradicar y recuperarse ante un incidente de seguridad, también establecer si el esquema de seguridad diseñado, es un escenario realista.

Por esto se realizarán ataques éticos, para contener ataques como exfiltraciónes o fugas de datos, esto por error de configuración, y se evaluara si la defensa activa mediante alertas simuladas en el SIEM, EDR o DLP, están configuradas acorde a lo que necesita la Secretaría, para lo que el ejercicio involucra al equipo técnico, líderes de proceso, comunicaciones y jurídico, siguiendo un protocolo que garantiza la seguridad del entorno y la preservación de evidencias.

El ciclo del simulacro incluye la detección del incidente, su análisis técnico, la contención operativa, la erradicación del vector de ataque y la recuperación segura de los sistemas que tiene como paso posterior la elaboración de un informe técnico con la causa raíz, impacto, línea de tiempo y acciones correctivas, para ajustar controles del SGSI, actualizando los riesgos, procedimientos y métricas, y fortaleciendo la resiliencia institucional frente a nuevas amenazas.

6.1.10. Plan de Comunicaciones y Capacitación Institucional.

El Plan de Comunicaciones y Capacitación Institucional tiene como propósito fortalecer la cultura organizacional en torno a la seguridad de la información y la protección de datos personales dentro de la Secretaría Distrital de Salud, para ello, se establecerán acciones estratégicas que permitan sensibilizar, formar y empoderar a todos los niveles de la entidad frente a sus responsabilidades en el manejo seguro de la información y su responsabilidad frente a la gestión Institucional.

En materia de comunicaciones, se desarrollarán campañas internas que promuevan buenas prácticas digitales, alertas sobre, riesgos latentes, riesgos potenciales y riesgos emergentes, y difusión de contenidos normativos clave mediante boletines, infografías, correos electrónicos y publicaciones en canales oficiales, para que estas acciones estén orientadas a mantener informada a la comunidad institucional sobre los riesgos en las actividades diarias, avances tecnológicos implementados, avances del Plan, los controles implementados y las recomendaciones vigentes.

La capacitación se estructurará en talleres presenciales y virtuales, enfocados en el cumplimiento de normas como la ISO/IEC 27001 de 2022, el MSPI y la legislación colombiana de protección de datos, en estas capacitaciones se abordarán temas como gestión de accesos, respuesta a incidentes, clasificación de información y uso seguro de tecnologías, además, se realizarán simulacros participativos que permitan validar el nivel de preparación institucional frente a auditorías y eventos críticos.

Pilar Gestión de Incidentes

6.1.11. Estrategia de Monitoreo, Respuesta y Aprendizaje

La detección tardía incrementa el impacto de los incidentes, por lo que el uso de herramientas de detección que permitan correlacionar eventos y detectar anomalías en tiempo real, estarán aplicándose en la vigencia de este plan.

Tener información suficiente, pertinente, veraz y oportuna, crea espacios claros para la toma de decisiones gerenciales, por lo que se deberá establecer una Mesa Técnica de Incidentes, como instancia decisoria, dirigida por la Dirección de Planeación Institucional y Calidad según la Resolución 1569 de 2024, en el artículo 26 y en conjunto con la dirección de TIC de la Secretaría Distrital de Salud y con la coordinación de referente de seguridad informática que establezca protocolos de acción basado en la Política General de Seguridad de la Información de la Secretaría, convoque a reuniones ordinarias y extraordinarias, que dirija el orden del día, coordine todo el ciclo de vida de los incidentes de seguridad informática y digital y deberá recibir y registrar los eventos que afectan la confidencialidad, integridad o disponibilidad de los datos e información, para proceder a analizarlos con el

propósito de determinar su origen, alcance, riesgos e impacto y aplicar medidas inmediatas de contención para reducir la afectación y deberá comunicar oportunamente a las áreas involucradas, supervisar la recuperación de los sistemas afectados y garantizar que se documenten las acciones y evidencias de manera trazable y conforme a normas como ISO 27001, 27701, MSPI y la legislación colombiana de protección de datos.

La Mesa Técnica de Incidentes definirá las acciones de intervención inmediata con el propósito de minimizar el riesgo de ocurrencia, proponer ajustes en políticas y controles para fortalecer la resiliencia institucional, la mejora continua, disminuir los ataques exitosos y asegurar que la entidad esté preparada para auditorías y futuros desafíos de seguridad.

El monitoreo actual se basa en prácticas reactivas y en el análisis manual de registros, lo que limita la capacidad de respuesta frente a incidentes complejos, por lo tanto, se requiere fortalecer el Centro de Operaciones de Seguridad SOC, interno o tercerizado, que permita correlacionar eventos generar alertas en tiempo real.

El plan incorpora tecnologías avanzadas como Análisis del Comportamiento de Usuarios y Entidades (UEBA) para detectar comportamientos que se salen de rangos normales de uso y se definirán protocolos de escalamiento y casos de uso que aseguran una gestión ordenada y trazable de los incidentes.

Gráfica No. 2 Ciclo de Vida de Incidentes de Seguridad de la Información.

6.2. Portafolio de Aplicaciones

El portafolio de aplicaciones constituye el instrumento operativo mediante el cual las estrategias de seguridad de la información se convierten en acciones concretas y medibles, por lo que cada aplicación debe contar con acciones para mitigar riesgos específicos sobre la confidencialidad, integridad y disponibilidad (CID) de los datos institucionales, alineándose con los controles de la ISO/IEC 27001 de 2022 y el

Modelo de Seguridad y Privacidad de la Información MSPI. Cada aplicación deberá garantizar que las acciones estén acompañadas de evidencias verificables como logs, alertas, reportes y se ajuste al ciclo de mejora continua PHVA, garantizar la trazabilidad, el cumplimiento normativo y la evolución constante frente a nuevas amenazas por que, en ese contexto, el portafolio se convierte en el puente entre la estrategia y la ejecución, garantizando que la seguridad de la información sea auditable, medible, sostenible y confiable.

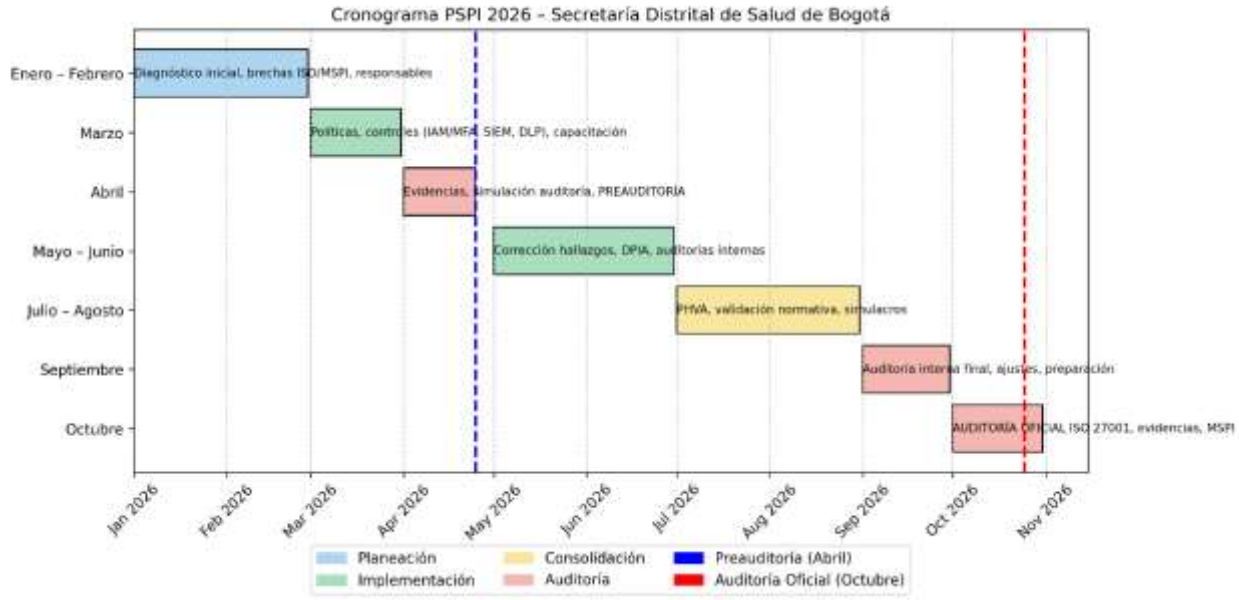
6.3. Cronograma de Actividades / Proyectos

El cronograma del Plan de Seguridad de la Información se organiza para garantizar la preparación institucional frente a la preauditoria que se efectuará en abril de 2026 y la auditoría de certificación en octubre de 2026 bajo la norma ISO/IEC 27001 de 2022.

En los primeros meses se realiza el diagnóstico de brechas y definición de proyectos (IAM/MFA, SIEM, DLP, CSPM) para que en marzo y abril se implementan controles iniciales y se consolidan evidencias para la preauditoria, que permitan identificar ajustes necesarios, para que entre mayo y agosto se ejecutan correcciones, se conformen evidencias del fortalecimiento de controles y auditorías internas, asegurando madurez operativa, llevando finalmente, en septiembre y octubre a cabo la validación final y preparación documental, culminando con la auditoría de certificación, donde se demuestra cumplimiento normativo, trazabilidad y mejora continua.

Mes / Periodo	Actividades principales	Documentos	Responsable
Enero – Febrero	Diagnóstico inicial, identificación de brechas ISO/MSPI, definición de portafolio, Desarrollo inicial del SoA, aplicación del plan de comunicaciones.	Lineamiento de Gestión de Incidentes - Mesa Técnica de Incidentes Plan de Auditoría Interna y Preauditoría Lineamiento de reacción Técnica frente a incidentes de seguridad.	Dirección de Planeación Institucional y Calidad. TIC
Marzo	Desarrollo de políticas, controles iniciales (IAM/MFA, SIEM, DLP), capacitación básica, definición final del SoA.	Declaración de Aplicabilidad (SoA) Inventario de Activos de Información y Tecnológicos. Política y Procedimientos de Control de Acceso (IAM/MFA). Presentación para Inicio de Capacitaciones.	Dirección de Planeación Institucional y Calidad. TIC Bienes y Servicio

Abril (hasta semana 4)	Consolidación de evidencias, simulación de auditoría interna, pre-auditoría oficial.		Dirección de Planeación Institucional y Calidad.
Mayo – Junio	Corrección de hallazgos, fortalecimiento de SIEM/DLP/CSPM, DPIA en procesos críticos, simulacros de incidentes, desarrollo de multifactor de autenticación MFA	Política de Criptografía y Gestión de Claves (TLS/KMS/HSM).	Dirección de Planeación Institucional y Calidad. TIC
Julio – Agosto	Integración PHVA, validación normativa, revisión documental.	Matriz de Riesgos de Seguridad y Privacidad.	Dirección de Planeación Institucional y Calidad. TIC
Septiembre	Preparación para auditoría externa, capacitación, Cierre de Planes de mejoramiento derivados de la Auditoría Interna.		Dirección de Planeación Institucional y Calidad.
Octubre (última semana)	Auditoría oficial ISO/IEC 27001:2022, entrega de evidencias, validación MSPI.	Informe de Auditoria Certificación	Dirección de Planeación Institucional y Calidad. TIC



6.4. Presupuesto

El presupuesto aproximado para la ejecución de este plan se encuentra alrededor de los SIETE MIL MILLONES CUATROCIENTOS DIEZ MILLONES SEISCIENTOS DOS MIL TRESCIENTOS DIECIOCHO PESOS (7.410.602.318)

7. Indicadores

La ausencia de indicadores claros y medibles ha sido una de las principales debilidades identificadas en evaluaciones previas del Sistema de Gestión de Seguridad y Privacidad de la Información, dificultando demostrar eficacia, eficiencia y mejora continua y que en coherencia con la ISO/IEC 27001 de 2022 y el MSPI, este Plan establece un sistema integral de indicadores orientado no solo al cumplimiento normativo, sino también a la toma de decisiones estratégicas por la Alta Dirección, basándose en la evidencia, por lo que los indicadores se estructuran en cuatro categorías, garantizando cobertura integral del ciclo PHVA.

- Estratégicos: %del avance de las mejoras o adaptaciones del desarrollo en las aplicaciones ejecutados dentro del cronograma (meta ≥ 90%).
- Operativos: Tiempo promedio de respuesta a incidentes de seguridad (meta ≤ 4 horas).
- De cumplimiento: % de controles del Anexo A de ISO/IEC 27001:2022 implementados y auditados (meta ≥ 95%).

Estos indicadores permiten medir el desempeño real del SGSPI, evaluar la efectividad de los controles, detectar desviaciones y riesgos emergentes, y soportar tanto la revisión por la dirección como las auditorías internas y externas.

8. SEGUIMIENTO

El seguimiento sistemático garantiza que el Plan de Seguridad y Privacidad de la Información (SGSPI) no se limite a un documento formal, sino que se traduzca en acciones verificables y medibles. Para ello, se establece un esquema integral que articula la gestión a través del Mesa de Seguridad y Privacidad de la Información, encargado de aprobar estrategias, priorizar riesgos, validar inversiones y supervisar la ejecución del SGSPI, evolucionando hacia un órgano con capacidad decisoria y soporte técnico especializado. El seguimiento se complementa con reportes periódicos: informes semestrales a la Alta Dirección y reportes mensuales de incidentes al área de Control Interno, respaldados por actas y registros como evidencia. Asimismo, se realizarán auditorías internas anuales y auditorías externas programadas, que permitirán verificar la conformidad y eficacia de los controles, en coherencia con el ciclo de mejora continua PHVA (Planear, Hacer, Verificar, Actuar).

Finalmente, se define un procedimiento de escalamiento institucional que asegura la atención oportuna de riesgos críticos: los incidentes graves serán elevados al Oficial de Seguridad y Alta Dirección, mientras que los riesgos altos serán gestionados directamente por el Comité Institucional de Gestión y Desempeño, garantizando trazabilidad, transparencia y capacidad de respuesta frente a amenazas emergentes.

8.1. Reportes y Comunicación

El sistema de reportes y comunicación asegura la trazabilidad y transparencia en la gestión del SGSPI, permitiendo a la Secretaría contar con información confiable y oportuna para la toma de decisiones, por esto se establecen dos mecanismos principales:

1. Informe SGSPI, dirigido a la Alta Dirección con una frecuencia trimestral y soportado en actas formales, que permite evaluar el avance de las estrategias y proyectos;
2. Reporte de Incidentes, remitido a la Mesa Técnica de Incidentes, que se convocará y dirigirá la Dirección de Planeación Institucional y Calidad cuando se presenten incidentes de seguridad, verificando los registros y soportes necesarios que faciliten el monitoreo de eventos de seguridad y la identificación de riesgos emergentes.

Estos reportes garantizan el cumplimiento de los requisitos de la ISO/IEC 27001 de 2022 y del MSPI, fortaleciendo la capacidad institucional de supervisión, respuesta inmediata y mejora continua.

8.2. Auditorias

Las auditorías constituyen un mecanismo esencial para verificar la conformidad, eficacia y mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI). En coherencia con la ISO/IEC 27001 de 2022 y el MSPI, se realizarán auditorías internas de carácter anual, donde estos ejercicios de verificación aportan evidencias objetivas, orientadas a evaluar el cumplimiento de políticas, procedimientos y controles desarrollados e implantados, generando hallazgos y planes de acciones correctivas y acciones de mejora, con el propósito de validar la alineación del SGSPI con los estándares internacionales y garantizar la preparación institucional para procesos de certificación que se llevaran a cabo el último trimestre del año 2026.

8.3. Escalamiento

El escalamiento asegura una respuesta oportuna y proporcional frente a incidentes y riesgos que puedan comprometer la seguridad de la información institucional, para

ello la entidad deberá dar cumplimiento al lineamiento de manejo de incidentes de seguridad de información.

9. Sustento Normativo

- ISO/IEC 27001:2022 – Norma internacional para gestión de seguridad de la información.
- ISO/IEC 27002:2022 – Código de buenas prácticas para controles de seguridad.
- ISO/IEC 22301:2019 – Norma para gestión de continuidad del negocio.
- Ley 1581 de 2012 – Régimen general de protección de datos personales.
- Ley 1712 de 2014 – Ley de Transparencia y Acceso a la Información Pública.
- Decreto 1078 de 2015 – Decreto Único Reglamentario del sector TIC (Gobierno Digital).
- Decreto 767 de 2022 – Actualiza el Decreto 1078, fortaleciendo Gobierno Digital y seguridad de la información.
- Resolución 500 de 2021 (MinTIC) – Adopta el Modelo de Seguridad y Privacidad de la Información (MSPI).
- Resolución 2277 de 2025 (MinTIC) – Refuerza obligatoriedad del ciclo PHVA en seguridad y privacidad.
- Resolución 705 de 2025 (SDS) – Política General de Seguridad de la Información de la Secretaría Distrital de Salud.
- Resolución 1569 de 2024 (SDS) – Define la Mesa Técnica de Incidentes y responsabilidades en gestión de seguridad.
- Política de Gobierno Digital (Decreto 1151 de 2008, Decreto 1008 de 2018) – Marco de transformación digital en entidades públicas.
- Modelo Integrado de Planeación y Gestión (MIPG) – Marco de gestión pública que integra seguridad de la información como componente de control interno.
- Esquema Nacional de Seguridad Digital (MinTIC) – Lineamientos para protección de datos y servicios digitales en el Estado.

10. Definiciones

Término	Definición	Traducción / Significado	Explicación
Activos de Información	Datos, documentos, sistemas y soportes que contienen información institucional	—	Comprende información física, digital, sensible y crítica que debe protegerse bajo principios de confidencialidad y reserva legal.
BCP	Business Continuity Plan	Plan de Continuidad del Negocio	Estrategia para mantener operaciones críticas ante incidentes.
BIA	Business Impact	Análisis de	Evalúa consecuencias de interrupciones

Término	Definición	Traducción / Significado	Explicación
	Analysis	Impacto al Negocio	en procesos críticos.
CID / CIA	Confidencialidad, Integridad y Disponibilidad (Confidentiality, Integrity, Availability)	Principios básicos de seguridad	Pilar fundamental de la seguridad de la información.
CISO	Chief Information Security Officer	Oficial/jefe de Seguridad de la Información	Responsable institucional de la estrategia de seguridad.
CSPM	Cloud Security Posture Management	Gestión de la Postura de Seguridad en la Nube	Evalúa y corrige configuraciones inseguras en servicios cloud remotas.
Dominio del Talento Humano y Tercerización	Ámbito que regula servidores públicos, contratistas y proveedores	—	Garantiza que todo el personal y terceros cumplan con estándares de seguridad y privacidad.
Dominio Procesal	Ámbito de aplicación del SGSI sobre procesos institucionales	—	Incluye procesos estratégicos, misionales, de apoyo y evaluación, garantizando seguridad en toda la cadena de valor.
Dominio Tecnológico e Infraestructura	Ámbito que cubre hardware, software, redes y servicios en la nube	—	Incluye infraestructuras críticas, dispositivos finales y servicios cloud bajo modelo de responsabilidad compartida.
DLP	Data Loss Prevention	Prevención de Pérdida de Datos	Conjunto de herramientas para evitar fugas de información sensible.
DRP	Disaster Recovery Plan	Plan de Recuperación ante Desastres	Define las estrategias para restaurar sistemas tras incidentes graves.
HSM	Hardware Security Module	Módulo de Seguridad de Hardware	Dispositivo físico para gestionar y proteger claves criptográficas.
IAM	Identity and Access Management	Gestión de Identidades y Accesos	Conjunto de políticas y tecnologías para asegurar que solo usuarios autorizados accedan a sistemas y datos.
IaaS	Infrastructure as a Service	Infraestructura como Servicio	Modelo de acceso remoto en la nube que provee servidores y almacenamiento virtualizados.
IDS	Intrusion Detection System	Sistema de Detección de Intrusiones	Detecta accesos no autorizados en redes, aplicaciones o sistemas.
IPS	Intrusion Prevention System	Sistema de Prevención de Intrusiones	Bloquea intentos de intrusión en tiempo real.
ISO/IEC 27001 de 2022	Norma internacional para gestión de seguridad de la información	International Organization for Standardization / International Electrotechnical Commission	Define un modelo compuesto de requisitos para establecer, desarrollar y mejorar un SGSI.

Término	Definición	Traducción / Significado	Explicación
ISO/IEC 27701	Extensión de ISO 27001 para gestión de privacidad	—	Añade controles específicos para el tratamiento de datos personales.
KMS	Key Management Service	Servicio de Gestión de Claves	Plataforma para administrar, rotar y auditar claves de cifrado.
MFA	Multi-Factor Authentication	Autenticación Multifactor	Uso de dos o más factores (contraseña, token, biometría) para validar identidad.
MIPG	Modelo Integrado de Planeación y Gestión	—	Marco de gestión pública colombiano que integra control interno, planeación y gestión institucional.
MSPI	Modelo de Seguridad y Privacidad de la Información	—	Marco colombiano del MinTIC que guía la implementación de estrategias para mejorar la seguridad y privacidad en entidades públicas.
PaaS	Platform as a Service	Plataforma como Servicio	Entorno en la nube para desarrollar y desplegar aplicaciones.
PHVA / PDCA	Ciclo de mejora continua: Planear, Hacer, Verificar, Actuar (Plan–Do–Check–Act)	—	Metodología para asegurar mejora continua en procesos de seguridad.
SaaS	Software as a Service	Software como Servicio	Aplicaciones listas para uso final (correo, colaboración, etc.).
SDS	Secretaría Distrital de Salud	—	Entidad pública responsable de la gestión de la salud en Bogotá, incluyendo la protección de datos ciudadanos.
SGSI	Sistema de Gestión de Seguridad de la Información	—	Marco de gestión para proteger la información institucional, basado en normas internacionales como ISO/IEC 27001.
SGSPI	Sistema de Gestión de Seguridad y Privacidad de la Información	—	Extiende el SGSI para incluir controles de privacidad, alineado con ISO/IEC 27701 y el MSPI.
SIEM	Security Information and Event Management	Gestión de Eventos e Información de Seguridad	Plataforma que centraliza registros y detecta anomalías en tiempo real.
SoA	Statement of Applicability	Declaración de Aplicabilidad	Documento ISO 27001 que define qué controles se aplican y por qué.
SOC	Security Operations Center	Centro de Operaciones de Seguridad	Unidad encargada de monitorear, detectar y responder a incidentes de seguridad.
SWG	Secure Web Gateway	Pasarela Segura de Internet	Filtra tráfico web para bloquear amenazas y accesos indebidos.
TLS	Transport Layer Security	Seguridad de la Capa de Transporte	Protocolo de cifrado para comunicaciones seguras en internet.
UEBA	User and Entity Behavior Analytics	Análisis de Comportamiento de Usuarios y Entidades	Tecnología que detecta anomalías en el comportamiento de usuarios y sistemas.

11. Control de Cambios

VERSIÓN	FECHA DE APROBACIÓN	RAZÓN DE ACTUALIZACIÓN
1	Enero de 2026	Se define el Plan de Seguridad y Privacidad de la Información y Protección de Datos Personales para la vigencia 2026.