PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA SECRETARÍA GENERAL DE LA ALCALDÍA MAYOR DE BOGOTÁ D.C.

Implementación y Mejora Continua del Modelo de Seguridad y Privacidad de la Información – MSPI (Sistema de Gestión de Seguridad de la Información – SGSI)

2026

Cra 8 No. 10-65
Código Postal 111711
Tel: +57 (601) 381 3000
www.secretariageneral.gov.co
Info: Línea 195

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA GENERAL

Contenido

Ilustraciones

Tablas

1. Introducción

La Secretaría General de la Alcaldía Mayor de Bogotá presenta a la ciudadanía, usuarios y grupos de interés el Plan de Seguridad y Privacidad de la Información correspondiente a la vigencia 2026, como parte de la implementación y mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI), también conocido como el Sistema de Gestión de Seguridad de la Información (SGSI).

Este plan ha sido actualizado para alinearse con la Norma Técnica Colombiana ISO/IEC 27001:2022, que introduce cambios clave en la gestión de riesgos, controles de seguridad y protección frente a amenazas emergentes.

La seguridad y privacidad de la información continúa siendo un pilar fundamental de la Política de Gobierno Digital, garantizando la mitigación de riesgos relacionados con la confidencialidad, integridad y disponibilidad de los activos críticos de la entidad. Este enfoque está orientado a proteger los intereses de la ciudadanía y asegurar la sostenibilidad de los servicios ofrecidos.

Con este plan, la Secretaría General de la Alcaldía Mayor de Bogotá reafirma su compromiso con la mejora continua y con la implementación de las mejores prácticas internacionales en la gestión de seguridad y privacidad de la información.

2. Objetivos

2.1 Objetivo general

Fortalecer el Modelo de Seguridad y Privacidad de la Información (MSPI) de la Secretaría General de la Alcaldía Mayor de Bogotá, alineándolo con los lineamientos de la norma ISO/IEC 27001:2022, con el fin de garantizar la protección

integral de los activos de información, mitigar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad, y asegurar la mejora continua de los procesos.

2.2 Objetivos específicos

- Fortalecer el estado actual del MSPI, identificando las brechas frente a los requisitos de la ISO/IEC 27001:2022 y proponer nuevos planes de acción.

- Adecuar e implementar controles de seguridad alineados con las áreas organizativas, tecnológicas, físicas y de personas definidas en la norma ISO/IEC 27001:2022.

- Fortalecer los procesos de identificación, evaluación y tratamiento de riesgos asociados con las amenazas emergentes y tecnologías disruptivas.

- Fortalecer el plan de sensibilización de seguridad y privacidad de la información, enfocándose en los cambios introducidos por la ISO/IEC 27001:2022.

- Establecer nuevos indicadores clave de desempeño (KPIs) para evaluar y optimizar continuamente la efectividad del MSPI.

3 Contexto estratégico

La Secretaría General de la Alcaldía Mayor de Bogotá reconoce que la información es uno de los activos más valiosos para garantizar la operación eficaz y la confianza de la ciudadanía. En este contexto, el Modelo de Seguridad y Privacidad de la Información (MSPI) se enmarca como un habilitador clave para el cumplimiento de

los objetivos estratégicos de la entidad adoptados mediante Resolución 630 de 2024[i], asegurando la alineación con la Norma ISO/IEC 27001:2022.

El contexto estratégico se define por:

Alineación con la Política de Gobierno Digital: Integración de los lineamientos de seguridad y privacidad de la información como parte de los pilares fundamentales para la transformación digital de la entidad.

Identificación de Grupos de Valor y Partes Interesadas: Análisis de las necesidades y expectativas de las partes interesadas, incluyendo ciudadanos, proveedores, contratistas y entidades regulatorias, para garantizar una gestión integral de la seguridad de la información conforme lo descrito en el documento Contexto estratégico [4202000-OT-066].

Gestión de Riesgos: Evaluación continua de riesgos asociados a la confidencialidad, integridad y disponibilidad de los activos de información, así como la identificación de oportunidades para fortalecer la seguridad, conforme se describe en el documento Guía metodológica para la gestión de riesgos de seguridad digital [4204000-GS-096].

Preparación para Amenazas Emergentes: Implementación de estrategias de protección frente a amenazas avanzadas. Actualmente en la entidad se define el proceso de atención de amenazas de seguridad digital conforme con lo descrito en el documento Gestión de incidentes de seguridad y privacidad de la información y gestión de vulnerabilidades [4204000-GS-042].

Sostenibilidad y Mejora Continua: Asegurar la sostenibilidad del MSPI mediante la mejora continua, el monitoreo de indicadores clave y la adaptación a los cambios en el entorno tecnológico y normativo.

Con este enfoque, el contexto estratégico del MSPI se convierte en un componente esencial para el cumplimiento de los objetivos institucionales y la protección de la información como activo crítico de la entidad.

4 Alcance

El Plan de Seguridad y Privacidad de la Información para la vigencia 2026 abarca todas las dependencias, procesos, sistemas de información, activos críticos y recursos humanos relacionados con la gestión de la información en la Secretaría General de la Alcaldía Mayor de Bogotá.

Su enfoque principal está orientado a:

- ✓ Protección de Activos de Información
- ✓ Gestión de Riesgos
- ✓ Cumplimiento Normativo
- ✓ Concienciación en todos los niveles de la entidad
- ✓ Mejora Continua

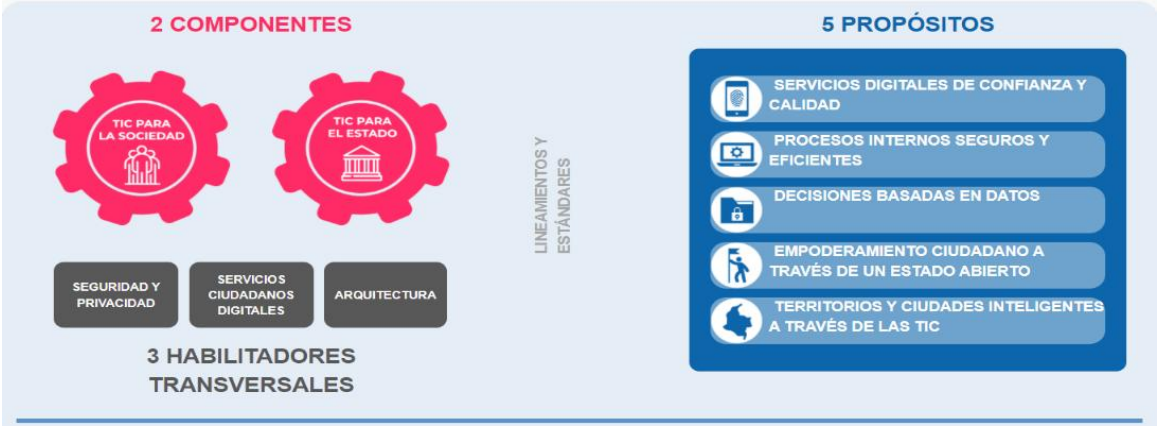
Este alcance asegura que todas las medidas adoptadas contribuyan al fortalecimiento de la gestión de la información como un recurso estratégico de la entidad, minimizando riesgos y garantizando la sostenibilidad de los servicios ofrecidos a la ciudadanía.

5 Operación del Modelo de Seguridad y Privacidad de la Información – MSPI (Sistema de Gestión de Seguridad de la Información – SGSI)

La operación del Modelo de Seguridad y Privacidad de la Información – MSPI (Sistema de Gestión de Seguridad de la Información – SGSI) en la Secretaría General de la Alcaldía Mayor de Bogotá está basada en la Política de Seguridad Digital, la cual constituye un pilar y uno de los habilitadores transversales definidos en la Política de Gobierno Digital. A continuación, se detalla el diagrama de la Política de Gobierno Digital, donde se detallan los componentes, habilitadores y propósitos de esta.

Ilustración 1 Elementos de la Política de Gobierno Digital

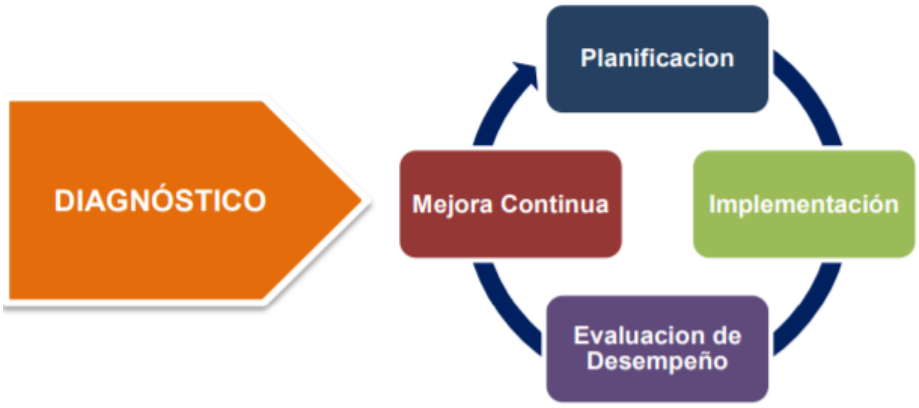
Fuente: *Gobierno Digital de MinTIC: https://gobiernodigital.MinTIC.gov.co/portal/Politica-de-Gobierno-Digital/*



El proceso de implementación del Modelo de Seguridad y Privacidad de la Información se fundamenta en el desarrollo del ciclo P – H – V – A: Planear – Hacer – Verificar – Actuar, tal como se indica en el modelo de operación del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, lo que permite que la seguridad y privacidad de la información sea un sistema de gestión sostenible al interior de la entidad, alineado con lo definido en la normatividad vigente.

Este enfoque asegura que el MSPI sea un sistema dinámico que responda a los riesgos emergentes y promueva una cultura organizacional centrada en la seguridad y privacidad de la información.

Ilustración 5. Ciclo de vida de operación del Sistema de Gestión de Seguridad de la Información – SGSI
Fuente: MinTIC: https://www.MinTIC.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf



6 Responsabilidad del Comité Institucional de Gestión y Desempeño

En el marco del cumplimiento de las políticas definidas en el Modelo Integrado de Planeación y Gestión – MIPG, y específicamente en lo referente a la política de seguridad digital, el artículo 2.2.2 de la Resolución 485 del 2024 define como función del Comité Institucional, asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información.

7 Sobre la Política de Seguridad de la Información y Seguridad Digital

La Resolución 373 de 2025, mediante la cual se adopta la Política de Seguridad de la Información y Seguridad Digital, se constituye en un referente obligatorio para la implementación del MSPI y para el desarrollo del presente plan. Entre los elementos más relevantes que se integran:

- La Política establece los criterios institucionales para la gestión segura de la información, asegurando la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.
- Define responsabilidades específicas para servidores públicos, contratistas y terceros, garantizando un marco de responsabilidad compartida en la protección de los activos de información.
- Establece el alcance institucional de la política, incluyendo infraestructura tecnológica, servicios, procesos, sedes y activos de información.
- Incorpora las obligaciones derivadas del Modelo de Seguridad y Privacidad de la Información y del marco normativo MinTIC.

8 Alineación del Plan con la Estrategia de Seguridad Digital

El Plan de Seguridad y Privacidad de la Información se encuentra plenamente alineado con la Estrategia de Seguridad Digital de la Secretaría General, adoptada mediante Resolución 373 de 2025, la cual constituye el instrumento marco que integra los principios, lineamientos, roles, mecanismos de gestión del riesgo, cultura de seguridad y controles aplicables a la Entidad.

La Estrategia establece:

- ✓ Principios orientadores como confidencialidad, integridad, disponibilidad, trazabilidad y mejora continua.
- ✓ La relación con el Plan de Acción Institucional y demás instrumentos de gestión
- ✓ La integración con arquitectura empresarial, procesos institucionales y el PETI 2025–2027.
- ✓ El modelo de gobernanza de seguridad digital definido por el Decreto Distrital 472 de 2024.

En consecuencia, las iniciativas, objetivos y actividades contempladas para la vigencia 2026 se desarrollan en coherencia con:

- ✓ El enfoque de gestión del riesgo digital.
- ✓ La articulación con el PETI, el PAI y el MSPI.
- ✓ El fortalecimiento de capacidades institucionales en cultura digital segura.
- ✓ La adopción progresiva de tecnologías emergentes

Con esta articulación, el Plan 2026 garantiza continuidad, coherencia y trazabilidad con la estrategia de seguridad digital.

9 Estado Actual de seguridad de la información en la entidad

Durante la vigencia 2025, la Secretaría General realizó el proceso de ajuste y transición del Modelo de Seguridad y Privacidad de la Información (MSPI) hacia los lineamientos establecidos en la norma ISO/IEC 27001:2022. Esta actualización

permitió fortalecer los controles de ciberseguridad, incorporar el enfoque basado en riesgos actualizados, y mejorar la capacidad institucional para responder a amenazas emergentes, incluyendo riesgos asociados a sistemas en la nube, servicios digitales esenciales y tecnologías disruptivas.

El diagnóstico y la evaluación del nivel de madurez del MSPI se consolidaron a partir del instrumento del MSPI, el cual evidencia que la Entidad mantiene un nivel Optimizado, con una efectividad del 96% en los controles aplicados. Este nivel de madurez refleja la consolidación de capacidades en:

- Gestión de activos
- Control de accesos
- Seguridad de las operaciones
- Continuidad del negocio

A continuación, y considerando el proceso de transición de la norma ISO 27001, se detalla el estado de la implementación bajo los dos instrumentos del MSPI versión 2013 y versión 2022.

Ilustración 2 Evaluación de efectividad de controles Versión 27001:2013

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	100	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	95	100	OPTIMIZADO
A.9	CONTROL DE ACCESO	100	100	OPTIMIZADO
A.10	CRIPTOGRAFÍA	90	100	OPTIMIZADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	100	100	OPTIMIZADO
A.12	SEGURIDAD DE LAS OPERACIONES	100	100	OPTIMIZADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	95	100	OPTIMIZADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	84	100	OPTIMIZADO
A.15	RELACIONES CON LOS PROVEEDORES	85	100	OPTIMIZADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	97	100	OPTIMIZADO
A.18	CUMPLIMIENTO	100	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		**96,11**	**100**	**OPTIMIZADO**

Ilustración 3 Brecha 27001:2013

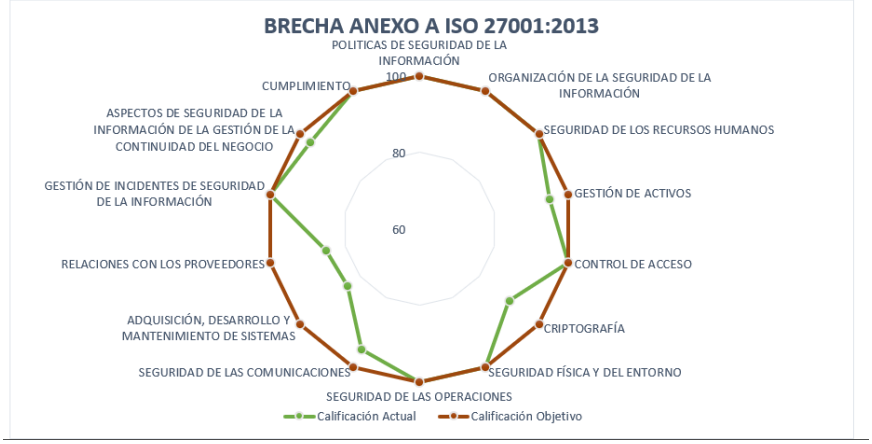
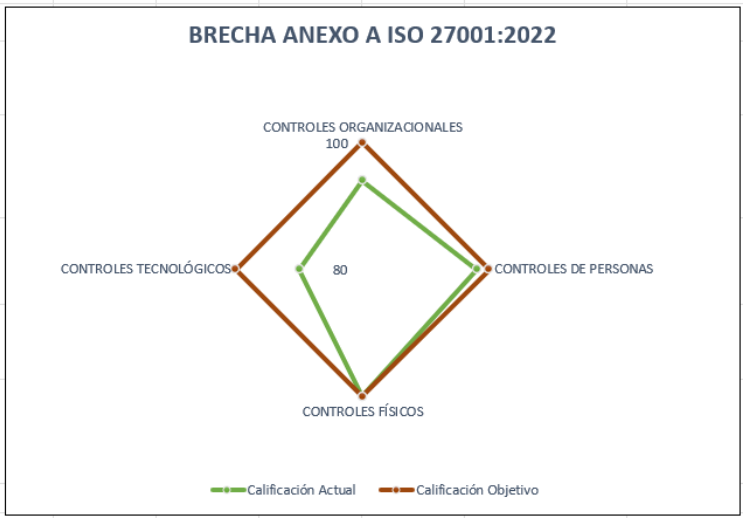


Ilustración 4 Evaluación de efectividad de controles ISO 27001:2022

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	Nivel de Madurez
A.5	CONTROLES ORGANIZACIONALES	94	100	OPTIMIZADO
A.6	CONTROLES DE PERSONAS	98	100	OPTIMIZADO
A.7	CONTROLES FÍSICOS	100	100	OPTIMIZADO
A.8	CONTROLES TECNOLÓGICOS	90	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		96	100	OPTIMIZADO

Ilustración 5 Brecha Anexo ISO 27001:2022



El estado consolidado de la gestión de seguridad y privacidad de la información con el que la Secretaría General finaliza la vigencia 2025, se detalla a continuación en los siguientes componentes claves de la estrategia de seguridad digital:

Gobernanza de Seguridad Digital

Durante la vigencia 2025 la Entidad fortaleció su modelo de gobernanza mediante:

- La consolidación de roles y responsabilidades documentadas en la Estrategia de Seguridad Digital.
- La operación de la Mesa Técnica de Apoyo en Archivo y Seguridad de la Información, como instancia asesora del Comité Institucional de Gestión y Desempeño.
- El seguimiento a auditorías, hallazgos y mejoras estructurales en cumplimiento del MSPI.
- La retroalimentación por parte del Comité Institucional de Gestión y Desempeño.

Estos avances permiten iniciar la vigencia 2026 con un modelo de gobernanza estable, documentado y con mecanismos de supervisión maduros.

Gestión de Activos de Información y Riesgos de seguridad

A continuación, se detalla el proceso de identificación, clasificación y valoración tanto de activos de información y riesgos para la vigencia 2025.

Ilustración 6 Distribución de Activos de Información

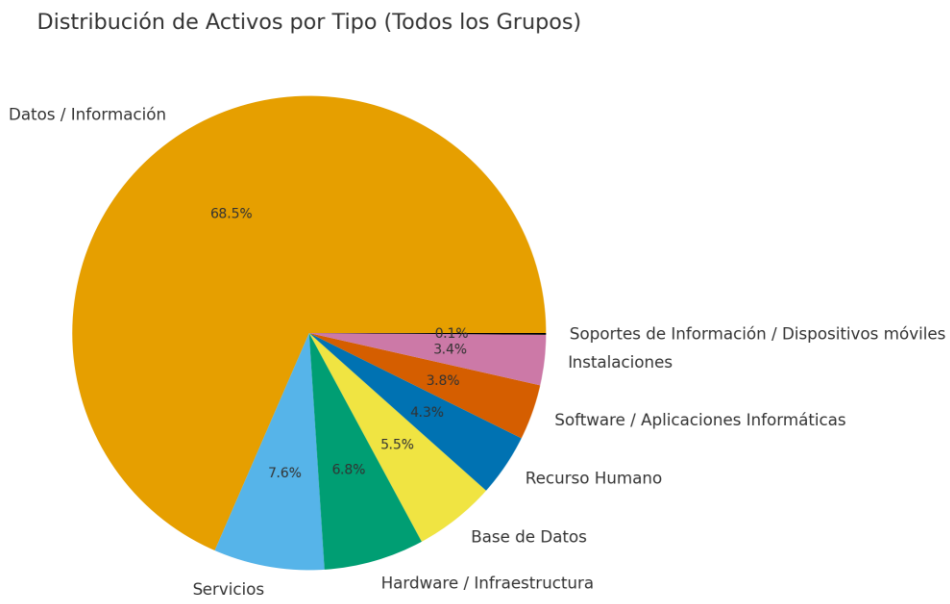


Ilustración 7 Criticidad de los Activos de Información

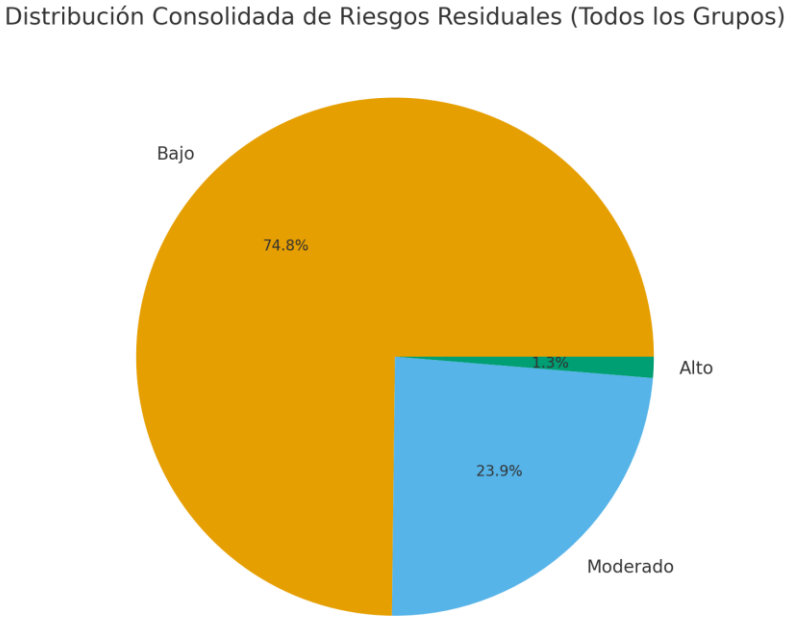
Como se evidencia en las gráficas anteriores, continúa siendo el activo tipo información, el más representativo, esto indica que la entidad gestiona altamente este activo especialmente en funciones:

- Jurídicas y disciplinarias
- Gestión documental
- Atención al ciudadano
- Procesos administrativos transversales

Los activos tecnológicos también representan una porción significativa (24%), lo que muestra dependencia de servicios TIC críticos para operación, continuidad y atención a la ciudadanía. Respecto a la criticidad de los activos, la mayoría se ubica en un nivel medio con un porcentaje del 49% y el 20% en un nivel alto; son estos activos a los que se le realiza el proceso de valoración de riesgos.

A continuación, se detalla el resultado de los riesgos residuales, de 532 riesgos consolidados:

Ilustración 8 Distribución Consolidada de Riesgos Residuales



Se indica que el sistema de control actual sí mitiga la mayoría de los riesgos, lo cual es positivo.

Sin embargo, 1 de cada 4 riesgos se mantiene en nivel moderado por lo tanto requiere fortalecimiento de controles.

Los 7 riesgos altos representan un riesgo institucional inmediato y deben tener plan de tratamiento obligatorio.

A continuación, se detalla la distribución en porcentaje de los riesgos residuales.

Concientización y Cultura de Seguridad

El fortalecimiento de la cultura institucional en seguridad digital constituye uno de los logros más relevantes de la vigencia 2025:

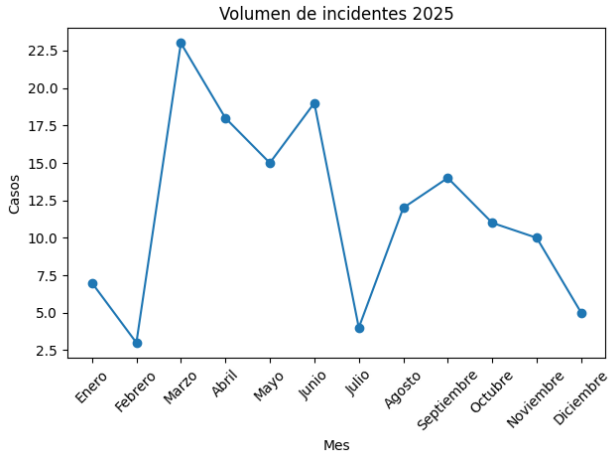
- Se ejecutó el **Plan de Sensibilización de Seguridad Digital 2025**, orientado a reforzar prácticas seguras en el manejo de la información, uso de tecnologías y reporte de incidentes.
- Se desarrollaron campañas temáticas y capacitaciones dirigidas a todos los servidores y contratistas.
- Se evaluó el impacto de las actividades de sensibilización, permitiendo ajustar el plan para la vigencia 2026.

El resultado es una mayor apropiación institucional de los principios de seguridad, impulsando la corresponsabilidad como elemento central del MSPI.

Gestión de Incidentes de Seguridad de la Información

La vigencia 2025 representó un año de alta exigencia para la gestión de incidentes de seguridad de la información, evidenciando un entorno operativo presionado por campañas externas, intentos de compromiso de cuentas institucionales, eventos de phishing, spoofing, enlaces maliciosos y actividad maliciosa recurrente sobre el correo corporativo.

Ilustración 9 Consolidado de Incidentes de Seguridad de la Información 2025



El consolidado anual permitió identificar un comportamiento cíclico y sostenido de riesgo, con picos relevantes en marzo y septiembre, y una tendencia de control progresivo en el segundo semestre gracias al fortalecimiento de medidas técnicas y operativas.

La gestión institucional alcanzó el cierre del 100% de los incidentes reportados, cumpliendo con la meta del indicador OTIC (≥90%), lo que refleja capacidad y disciplina operativa. Sin embargo, el análisis demuestra que la entidad aún se

encuentra en un nivel de madurez reactivo–controlado, dependiendo parcialmente de la notificación del usuario y de acciones derivadas del incidente, más que de mecanismos de monitoreo preventivo o correlación avanzada.

En términos técnicos, la adopción de controles como MFA, DMARC, SPF, DKIM, bloqueo geográfico, sandbox y medidas puntuales de endurecimiento contribuyeron a estabilizar el riesgo, pero requieren continuidad, estandarización y gobierno formal. La implementación de la solución de XDR y el respectivo monitoreo deberá apoyar el proceso para la siguiente vigencia 2026.

La dimensión humana sigue siendo determinante: cuando el usuario reporta, el riesgo se mitiga; cuando no lo hace, el riesgo escala. Esto confirma la necesidad de un programa permanente de sensibilización basado en incidentes reales, no campañas aisladas.

Finalmente, el comportamiento anual reafirma la necesidad de continuar articulando la gestión de incidentes con la continuidad de negocio (DRP/BCP), infraestructura, gobierno tecnológico y toma de decisiones directivas. La seguridad no puede operar como respuesta puntual o aislada: debe consolidarse como un componente estructural de la gestión pública, presupuestal y estratégica.

Fortalecimiento de la Infraestructura Tecnológica

Con base en el PETI 2025–2027 y la Estrategia de Seguridad Digital, se ejecutaron actividades orientadas al fortalecimiento de la infraestructura de TI, destacándose:

- Actualización y aseguramiento progresivo de plataformas tecnológicas críticas.
- Implementación de nuevos controles de seguridad para prevenir la materialización de riesgos en los servicios de la entidad.

- Evaluación y mitigación de vulnerabilidades en sistemas críticos d la entidad.
- Avances en la adopción de tecnologías seguras y arquitectura empresarial.

Estos esfuerzos se enmarcan en el objetivo de evitar la materialización de riesgos de seguridad digital y asegurar la continuidad de los servicios institucionales.

Finalmente, para la vigencia 2026, la entidad busca cerrar brechas identificadas en los anexos comparativos con la ISO/IEC 27001:2022 e implementar nuevos controles aplicables a riesgos tecnológicos emergentes, ciberamenazas en expansión y servicios digitales estratégicos para la operación de la Entidad.

10 Plan de trabajo del Sistema de Gestión de Seguridad de la Información

El plan de trabajo diseñado para ser revisado y aprobado tanto por la Jefatura de la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC), como por el Comité Institucional de Gestión y Desempeño es el siguiente:

Tabla 1: Plan de trabajo implementación del MSPI (Sistema de Gestión de Seguridad de la Información – SGSI) – Fuente: Elaboración propia

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VIGENCIA 2025						
N.	FASE	ACTIVIDADES	DEPENDENCIA RESPONSABLE	PRODUCTO / ENTREGABLE	FECHA INIC	FECHA FI
1	PLANEACIÓN	Definición de actividades detalladas del plan inicial de seguridad y privacidad de la Información para la vigencia 2026	OTIC	Plan de seguridad y privacidad de la información 2026	ENERO	JULIO
2		Definciión de actividades detalladas del plan de sensibilización y comunicaciones de seguridad y privacidad de la Información para la vigencia 2026	OTIC	Plan de sensibilización y comunicación de seguridad y privacidad de la información - vigencia 2026, alineado al Plan de Comunicaciones de la Secretaría General de la Alcaldía Mayor de Bogotá	ENERO	FEBRERO
3		Elaborar plan inicial de seguridad y privacidad de la Información para la vigencia 2027	OTIC	Plan Inicial de seguridad y privacidad de la información 2027	NOVIEMBRE	DICIEMBRE
4		Elaborar propuesta inicial del plan de sensibilización y comunicación de seguridad y privacidad de la Información para la vigencia 2027	OTIC	Plan Inicial de sensibilización y comunicación de seguridad y privacidad de la información - vigencia 2027, alineado al Plan de Comunicaciones de la Secretaría General de la Alcaldía Mayor de Bogotá	NOVIEMBRE	DICIEMBRE
5-6	IMPLEMENTACIÓN	Implementar controles para el fortalecimiento del Programa Integral de Datos Personales	OTIC	Actividades realizadas para el fortalecimiento del Programa Integral de Datos Personales	ENERO	NOVIEMBRE
7-8		Implementar controles para el fortalecimiento del Modelo de Seguridad y Privacidad de la Información	OTIC	Actividades realizadas para el fortalecimiento del Modelo de Seguridad y Privacidad de la Información	MARZO	NOVIEMBRE
9		Actualizar los activos de información, riesgos de seguridad digital y planes de tratamiento de riesgos asociados.	OTIC	Activos de información, riesgos de seguridad digital y planes de tratamiento de riesgos actualizados / Registro de Activos de información e índice de información clasificada publicados	FEBRERO	DICIEMBRE
10		Implementar controles para el fortalecimiento de la infraestructura tecnológica de la Entidad	OTIC	Actividades realizadas para el fortalecimiento de la infraestructura tecnológica de la Entidad	ENERO	DICIEMBRE
11		Implementar el DRP para los servicios críticos priorizados en la entidad		DRP implementado para los servicios priorizados en la entidad	MARZO	DICIEMBRE
12		Fortalecer la cultura de seguridad y privacidad de la información al interior de la Entidad	OTIC	Actividades realizadas para el fortalecimiento de la cultura de seguridad y privacidad de la información al interior de la Entidad	FEBRERO	DICIEMBRE
13		Realizar revisión de los controles de la Norma ISO 27001:2022 (conforme a brecha)	OTIC	Informe de seguimiento de controles definidos en el alcance de la vigencia 2026	MARZO	NOVIEMBRE
14	SEGUIMIENTO	Realizar seguimiento a los riesgos de seguridad de la información y/o seguridad digital	OTIC	Evidencias de seguimiento a los riesgos de seguridad de la información y/o seguridad digital	ENERO	AGOSTO
15		Atender los requerimientos del Modelo Integrado de Planeación y Gestión -.MIPG y FURAG, relacionados con la implementación de la política de seguridad digital	OTIC	Actividades de apoyo realizadas para el cumplimiento del Modelo Integrado de Planeación y Gestión (MIPG), FURAG / Auditorias recibidas en la OTICs relacionadas con seguridad digital	MAYO	DICIEMBRE
16		Realizar seguimiento a los indicadores del MSPI	OTIC	Reporte de seguimiento a Indicadores	ENERO	DICIEMBRE
17	MEJORA CONTINUA	Actualizar autodiagnóstico seguridad de la información y el diagnóstico de datos personales de acuerdo con lo establecido por MINTIC	OTIC	Autodiagnóstico de seguridad de la información - Diagnóstico de Datos personales de acuerdo con lo establecido por MINTIC actualizado	MAYO	DICIEMBRE

11 Marco Normativo

A continuación, se detalla el marco normativo sobre el cual se basó el desarrollo del presente plan se nombra a continuación:

- **Constitución Política de Colombia de 1991**: Artículo 15,20
- **Ley 1273 de 2009**: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- **Ley 1581 de 2012**. Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Ley 1712 de 2014**. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- **Decreto 886 de 2014**. Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
- **Decreto 103 de 2015**. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- **Decreto 1008 del 2018**. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 338 de 2022**: Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad

digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.

- **Decreto 472 de 2024:** Por el cual se adopta el Modelo de Gobernanza de Seguridad Digital para el Distrito, se modifica el artículo 5 del Decreto Distrital 025 de 2021 y se dictan otras disposiciones.
- **Resolución 777 de 2019.** Por la cual se adopta la Política de Privacidad y Tratamiento de Datos Personales y el "Manual de Políticas y Procedimientos para el Tratamiento de Datos Personales" de la Secretaría General de la Alcaldía Mayor de Bogotá, D. C., y se deroga la Resolución 070 de 2017.
- **Resolución 500 de 2021:** Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
- **Resolución No. 485 de 2024**: Por la cual se actualiza la reglamentación del Comité Institucional de Gestión y Desempeño en la Secretaría General de la Alcaldía Mayor de Bogotá, D.C. y se sustituyen unos Capítulos del Título II de la Resolución 728 de 2023 “Por la cual se unifica y actualiza la reglamentación de las instancias internas de coordinación en la Secretaría General de la Alcaldía Mayor de Bogotá, D.C."
- **Resolución 2277 de 2025**. Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.

- **Resolución 373 de 2025** Por la cual se adopta la Política de Seguridad de la Información y Seguridad Digital y la Estrategia de Seguridad Digital de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C

- **CONPES 3701 de 2011**: Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- **CONPES 3854 de 2016**: Política Nacional de Seguridad digital.

- **Conpes 3975 de 2019:** Política Nacional para la Transformación Digital e Inteligencia Artificial
- **Conpes 3995 de 2020:** política Nacional de Seguridad y Confianza Digital

12 Documentos de referencia

- **Política de Gobierno Digital** - Modelo de Seguridad y Privacidad de la Información (MSPI) – MinTIC.
- **Manual Operativo del Modelo Integrado de Planeación y Gestión.**
- Norma Técnica Colombiana ISO 27001:2022.

13 Aprobaciones y Control de Cambios

13.1 Aprobaciones

El presente documento fue creado, revisado, modificado y aprobado por:

	NOMBRE	CARGO	FECHA
ELABORÓ	Lourdes María Acuña Acuña	Contratista	Noviembre/2025
REVISÓ	Erika Tatiana Quintero Quintero	Contratista	Diciembre/2025
	Arleth Patricia Saurith Contreras	Jefe Oficina de Tecnologías de la Información y las Comunicaciones – OTIC	Diciembre/2025
APROBÓ	Comité Institucional de Gestión y Desempeño	Comité Institucional de Gestión y Desempeño	Enero/2026

13.2 Control de Cambios

ASPECTOS QUE CAMBIARON EN EL DOCUMENTO	DETALLE DE LOS CAMBIOS EFECTUADOS	FECHA DEL CAMBIO	VERSIÓN
N/A	Creación del documento	21/04/2020	1.0
Introducción, objetivo, alcance, contexto estratégico Plan de implementación del	Modificación del texto de la introducción, objetivo, Alcance. Texto Plan Acción Integrado 2021. Actualización del Plan por	26/01/2021	2.0

ASPECTOS QUE CAMBIARON EN EL DOCUMENTO	DETALLE DE LOS CAMBIOS EFECTUADOS	FECHA DEL CAMBIO	VERSIÓN
Modelo de Seguridad y Privacidad de la Información.	cambio de vigencia a 2021. Modificación del cronograma correspondiente al Plan de implementación para el habilitador de Seguridad y Privacidad de la Información.		
Introducción, objetivo, alcance. Contexto estratégico. Plan de implementación del Modelo de Seguridad y Privacidad de la Información.	Modificación del texto de la introducción, objetivo, alcance. Texto Plan Acción Integrado 2022. Actualización del Plan por cambio de vigencia a 2021. Modificación del cronograma correspondiente al Plan de implementación para el habilitador de Seguridad y Privacidad de la Información.	17/01/2022	3.0
Introducción, objetivo, alcance. Contexto estratégico. Plan de implementación del	Modificación del texto de la introducción, objetivo, alcance. Texto Plan Acción Integrado 2023.	18/01/2023	4.0

ASPECTOS QUE CAMBIARON EN EL DOCUMENTO	DETALLE DE LOS CAMBIOS EFECTUADOS	FECHA DEL CAMBIO	VERSIÓN
Modelo de Seguridad y Privacidad de la Información.	Actualización del Plan por cambio de vigencia a 2022. Modificación del cronograma correspondiente al Plan de implementación para el habilitador de Seguridad y Privacidad de la Información.		
Comité de Seguridad y privacidad de la información – Plan de Implementación del Modelo de Seguridad y Privacidad de la Información.	Se incluye información relacionada con la mesa técnica de archivo y seguridad de la información. Se actualiza el plan a la vigencia 2023	16/03/2023	5.0
Actualización general del documento	Se actualiza el plan a la vigencia 2024	28/12/2023	6.0
Actualización general del documento	Se actualiza el plan a la vigencia 2025	15/01/2025	7.0
Actualización general del documento	Se actualiza el plan a la vigencia 2026	Enero/2026	8.0

¡ ***Por la cual se adopta la plataforma estratégica de la Secretaría General de la Alcaldía Mayor de Bogotá, D. C. y se deroga la Resolución 277 de 2020***"