ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA DISTRITAL DE LA MUJER

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - 2026

PROCESO GESTIÓN TECNOLÓGICA

Bogotá, D.C., enero 2026

Contenido

1. INTRODUCCIÓN

El Modelo de Seguridad y Privacidad de la Información - MSPI, actualizado mediante la Resolución MinTIC 02277 de 2025, es el instrumento a través del cual el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC establece los lineamientos que deben seguir las entidades públicas en cumplimiento de la política de gobierno digital en su habilitador transversal "Seguridad de la información".

La Secretaría Distrital de la Mujer completó exitosamente durante 2025 la transición del Sistema de Gestión de Seguridad de la Información (SGSI) de la norma ISO 27001:2013 a ISO 27001:2022, cumpliendo con el plazo crítico internacional (31 de octubre de 2025). Este logro posiciona a la entidad como referente en el sector público colombiano, demostrando madurez en la gestión de seguridad de la información.

El Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018, en el artículo 2.2.9.1.1.3. define la seguridad de la información como principio de la Política de Gobierno Digital. La implementación del Plan de Seguridad y Privacidad de la Información obedece a las necesidades objetivas, requisitos y acciones en materia de seguridad, promoviendo la implementación y apropiación de las mejores prácticas definidas en el MSPI y en el estándar ISO 27001:2022.

La Política General de Seguridad de la Información de la Entidad fue actualizada mediante el documento GT-PLT-1, la cual se encuentra en aprobación y está incorporando las nuevas directrices del estándar internacional y estableciendo el marco de referencia para todos los instrumentos del sistema.

2. OBJETIVO GENERAL

Establecer actividades que permitan proteger la confidencialidad, integridad y disponibilidad de la información sensible y personal gestionada por la SDMujer, a través de la implementación de prácticas de seguridad de la información alineadas con ISO 27001:2022, la capacitación continua del personal y la adopción de tecnologías que aseguren el cumplimiento de las normativas legales vigentes, con el fin de garantizar un entorno seguro y confiable para todas las partes involucradas.

3. OBJETIVOS ESPECÍFICOS

- Consolidar la implementación del Sistema de Gestión de Seguridad de la Información conforme a ISO 27001:2022 y el MSPI actualizado (Resolución 02277 de 2025).
- Establecer actividades para dar continuidad al desarrollo y mejora del sistema de gestión de seguridad en la Secretaría Distrital de la Mujer.
- Fortalecer las capacidades de detección, respuesta y recuperación ante incidentes de seguridad.
- Consolidar el inventario de activos de información y la trazabilidad riesgo-activo-control.

4. ALCANCE

El Plan de Seguridad y Privacidad de la Información aplica para la vigencia 2026 a todos los niveles de la Entidad en cumplimiento de sus funciones, así como a servidoras, servidores públicos y contratistas en Nivel Central, Casas de Igualdad de Oportunidades para las Mujeres, Casa Refugio, Casa de Todas, en las cuales se genere, acceda, almacene, comparta, procese o transmita información de la Entidad o beneficiarias, ya sea en medios físicos, electrónicos, haciendo uso de la infraestructura tecnológica provista por la entidad o de propiedad de sus contratistas.

5. DEFINICIONES

- **Activo de Información:** Datos o conocimiento que tienen valor para una organización.
- **Alta dirección:** Persona o grupo de personas que dirige y controla una organización, al nivel más alto
- **Amenaza:** Causa potencial de un incidente no deseado, que puede resultar en daños a un sistema u organización.
- **BIA (Business Impact Analysis / Análisis de Impacto en el Negocio):** Proceso de análisis de las actividades de una organización y del efecto que una interrupción del negocio podría tener sobre ellas. Permite identificar qué procesos son críticos y qué tiempos de recuperación se requieren.
- **Clasificación de la información**: Los responsables de los activos de información deben documentar la clasificación de seguridad de los activos de información de los cuales son responsables y designarán un custodio para cada activo, a su vez éste será responsable de la implementación de los controles de seguridad.
- **Confidencialidad:** Propiedad para que la información no esté disponible o divulgada a personas, entidades o procesos no autorizados.
- **Control:** Medida que modifica el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizativas.
- **Custodio:** Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado. Tomado de https://www.mintic.gov.co/gestionti/615/articles-482 G5_Gestion_Clasificacion.pdf
- **Dato Personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables (Ley 1581 de 2012 — Artículo 3).
- **Disponibilidad:** Propiedad de la información relacionada con ser accesible y utilizable a petición de una entidad autorizada.
- **DLP (Data Loss Prevention / Prevención de Fuga de Datos):** Conjunto de herramientas y políticas diseñadas para detectar y prevenir que la información

sensible salga de la organización de manera no autorizada o sea accedida por usuarios indebidos.

- **Evento de seguridad de la información:** Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o falla de salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.
- **Gestión de riesgos:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **Hardware:** Conjunto de equipos de cómputo, servidores, redes, equipos de seguridad, impresoras, scanner, equipos de almacenamiento, entre otros, que utiliza la Secretaría Distrital de la Mujer.
- **Impacto:** La magnitud del daño que se puede esperar como resultado de la divulgación, modificación no autorizada, destrucción, o pérdida de información.
- **Incidente de seguridad de la información:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Información:** Es un conjunto de datos ordenados, clasificados y almacenados en cualquier medio (magnético, papel, correo electrónico, conversación telefónica, chat, USB, etc.).
- **Información documentada:** Información requerida para ser controlada y mantenida por una organización y el medio en el que está contenida. La información documentada puede estar en cualquier formato y medio y desde cualquier fuente y puede referirse al sistema de gestión (incluidos los procesos relacionados), información creada para que la organización funcione (documentación) y/o evidencias de resultados alcanzados (registros)
- **Incidente:** Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Matriz RACI:** Herramienta de gestión de proyectos que se utiliza para aclarar roles y responsabilidades en tareas o procesos. Sus siglas corresponden a: **R**esponsable

(quien hace la tarea), **A**ccountable (quien rinde cuentas/aprueba), **C**onsulted (a quien se consulta) e **I**nformed (a quien se informa).

- **MSPI:** Modelo de Seguridad y Privacidad de la Información establecido por MinTIC.
- **On-premise:** Modelo de implementación de software o infraestructura donde los sistemas se ejecutan en las instalaciones físicas de la organización (servidores propios), en contraposición a los servicios en la nube.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.
- **RNBD (Registro Nacional de Bases de Datos):** Directorio público operado por la Superintendencia de Industria y Comercio donde se inscriben las bases de datos sujetas a tratamiento de datos personales en Colombia.
- **RTO (Recovery Time Objective / Tiempo Objetivo de Recuperación):** Período de tiempo tras un incidente dentro del cual se debe reanudar un producto o actividad, o se deben recuperar los recursos, para evitar impactos inaceptables.
- **RPO (Recovery Point Objective / Punto Objetivo de Recuperación):** Punto en el tiempo al que deben recuperarse los datos o actividades después de una interrupción (determina la pérdida máxima tolerable de datos).
- **Propietario de la Información**: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso.
- **SIEM (Security Information and Event Management):** Solución tecnológica que centraliza el almacenamiento y análisis de los registros (logs) de seguridad generados por diferentes activos (firewalls, servidores, antivirus), permitiendo la detección de amenazas y respuestas ante incidentes en tiempo real.
- **Sistema de información:** Aplicaciones, servicios, activos de tecnología de la información u otros componentes de manejo de información.
- **SGSI - Sistema de Gestión de Seguridad de la Información:** Sistema de Gestión de Seguridad de la Información basado en ISO 27001:2022.

- **Seguridad de la Información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas.
- **SoA:** Statement of Applicability (Declaración de Aplicabilidad) - Documento que describe los controles aplicables al SGSI.
- **SAST (Static Application Security Testing):** Es un análisis de **"Caja Blanca"**. Revisa el código fuente de la aplicación desde adentro y sin ejecutarla para encontrar errores de programación en busca de vulnerabilidades de seguridad sin necesidad de ejecutar el programa. Permite la identificación temprana de defectos en el ciclo de vida de desarrollo (SDLC).
- **DAST (Dynamic Application Security Testing):** Es un análisis de **"Caja Negra"**. Prueba la aplicación desde afuera mientras está en ejecución, estas pruebas validan el comportamiento del software frente a entradas específicas (incluyendo entradas maliciosas) comparando los resultados reales con los esperados.
- **Software:** Conjunto de programas, sistemas operativos, aplicaciones de ofimática entre otros aplicativos propios y/o tercerizados que utiliza la Secretaría Distrital de la Mujer.
- **Terceros:** Personas que no son empleados de la Secretaría Distrital de la Mujer o empresas diferentes al mismo. Ejemplo: Participantes, beneficiarios, proveedores regulares o potenciales de bienes y servicios, empresas candidatas a prestar servicios a la Secretaría Distrital de la Mujer, entes reguladores, consultores, etc.
- **Vulnerabilidad:** Debilidad de un activo o de un control que puede ser explotada por una o más amenazas (ISO/IEC 27000:2018, cláusula 3.77).

6. DESARROLLO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El desarrollo del Plan de Seguridad de la Información de la Secretaría Distrital de la Mujer está basado en la aplicación del ciclo PHVA (Planear, Hacer, Verificar y Actuar), de acuerdo con las directrices del MSPI 2025 (Resolución 02277), ISO 27001:2022 y el Decreto 1008 del 14 de junio de 2018.

Tabla 1. *Ciclo PHVA*

Fase	Descripción
PLANIFICAR	Actualizar y/o definir la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar los activos y el riesgo.
HACER	Implementar y operar la política, los controles, procesos y procedimientos del SGSI.
VERIFICAR	Evaluar y medir el desempeño del proceso contra la política y los objetivos de seguridad.
ACTUAR	Establecer acciones correctivas y preventivas para lograr la mejora continua.

Elaboración Oficina Asesora de Planeación, 2026.

Contexto 2025 - Base para el Plan 2026

Durante 2025 la Secretaría Distrital de la Mujer completó la transición a ISO 27001:2022, logrando:

- Declaración de Aplicabilidad (SoA v3): Evaluación de 93 controles con justificación de inclusión/exclusión.
- 11 nuevos controles ISO 27001:2022: Incorporados controles para servicios en la nube (5.23), inteligencia de amenazas (5.7), continuidad TIC (5.30), eliminación segura (8.10), enmascaramiento de datos (8.11), prevención de fuga de datos (8.12), entre otros.
- Gestión de incidentes: Se gestionaron exitosamente incidentes en INFOCUIDADO, SIMISIONAL, ORFEO y OMEG.
- Manual de Políticas Específicas (GT-MA-3 v5): Documentación de políticas para los nuevos controles de seguridad.

7. ACTIVIDADES DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para la definición de las actividades del plan institucional de seguridad de la información para la vigencia 2026, se tuvo en cuenta:

- El informe de auditoría MSPI de 2025
- La transición completada a ISO 27001:2022
- El nivel de madurez de controles de seguridad de datos personales
- El seguimiento al plan ejecutado durante 2025
- Los riesgos identificados de seguridad de la información

Actividades 2026

Las actividades para 2026 incorporan las **oportunidades de mejora** identificadas en la Auditoría Interna MSPI y AE (Radicado 3-2025-004948), alineadas con los **nuevos controles de ISO 27001:2022**.

Indicador de Eficacia: El cumplimiento de cada actividad se mide como:

(Avance reportado / Meta 2026) × 100%

El porcentaje de avance se calcula según la naturaleza del producto: para actividades con entregables únicos corresponde al grado de completitud; para actividades con componentes múltiples (ej. DLP) se calcula como la proporción de elementos implementados sobre el total programado.

Es importante mencionar que existen actividades que son recurrentes cada año y por tanto inician con un porcentaje de 0, ejemplo la actividad 1.2 de la tabla 2.

Tabla 2. *Actividades 2026*

No.	ACTIVIDAD	PRODUCTO	FECHA FIN	RESPONSABLE	META 2026	CONTROL ISO 27001:2022
1. DATOS PERSONALES						
1.1	Desarrollar actividades del Plan de protección de datos personales	Informes de actividades del	15-dic-2026	Grupo interdisciplinario	0% → 100%	5.34

		grupo interdisciplinario				
1.2	Realizar registro en el RNBD del inventario de bases de datos personales	Inventario actualizado en RNBD	30-jun-2026	Despacho, OAP, OAJ	0% → 100%	5.12
1.3	Capacitar al personal en tratamiento de datos personales	Registros de capacitaciones	30-dic-2026	OAP	0% → 100%	6.3
2. INFORMACIÓN DOCUMENTADA						
2.1	Publicar políticas de seguridad actualizadas en SIG	GT-PLT-1 v4 y GT-MA-3 v5 publicados	31-mar-2026	Despacho, OAP, OAJ	95% → 100%	5.1
2.2	Documentar matriz RACI de seguridad de la información	Matriz RACI publicada en SIG	30-sep-2026	OAP y dependencias	75% → 90%	5.2, 5.3
2.3	Publicar cambios en formato de procedimiento de activos con formato MinTIC	Formato de activos de información publicado en SIG	30-jun-2026	OAP, DAF, OAJ	95% → 100%	5.9
2.4	(OM-05/OM-08) Socializar políticas de eliminación segura y trazabilidad de administradores (ya documentadas en GT-MA-3 v5)	Registros de socialización y evidencias de aplicación	30-sep-2026	OAP	0% → 100%	8.10, 8.15
2.5	(OM-09) Formalizar Guía de Desarrollo Seguro en Kawak	GT-GU-3 publicada en SIG	30-jun-2026	OAP, DGC	0% → 100%	8.28
3. ACTIVOS DE INFORMACIÓN						
3.1	Actualizar activos de información e índice clasificada/reservada	Inventario publicado en página web	15-dic-2026	OAP, DAF, dependencias	0% → 100%	5.9
3.2	Consolidar trazabilidad riesgo-activo-control	Matriz de trazabilidad implementada	31-ago-2026	OAP, DAF	0% → 100%	5.9, 5.10
4. RIESGOS Y CONTINUIDAD						
4.1	Seguimiento cuatrimestral a planes de tratamiento de riesgos	3 informes de seguimiento en SIG	31-dic-2026	OAP y dependencias	0% → 100%	5.5
4.2	(OM-02) Evaluar opciones para la implementación de solución SIEM institucional para monitoreo de activos críticos on-premise	Informe técnico	30-ago-2026	OAP	0% → 100%	8.16

4.3	Completar etiquetado DLP en SharePoint/OneDrive y SearchInform	Configuraciones DLP operativas	30-sep-2026	OAP	0% → 50%	8.12
4.4	(OM-03) Desarrollar guías de contingencia para sistemas críticos según BIA	Guías con RTO/RPO definidos	30-sep-2026	OAP, DGC	0% → 100%	5.30
4.5	(OM-06) Socializar política de enmascaramiento (GT-MA-3 v5) y evaluar implementación en sistemas críticos	Registros de socialización e informe de viabilidad técnica	31-oct-2026	OAP, DGC	0% → 100%	8.11
4.6	Actualizar BIA con nuevos servicios críticos	BIA actualizado	30-nov-2026	OAP, dependencias	0% → 100%	5.30
4.7	Elaborar informe de lecciones aprendidas incidentes 2025	Informe consolidado (INFOCUIDADO, SIMISIONAL, ORFEO, OMEG)	31-mar-2026	OAP	0% → 100%	5.27
4.8	Realizar análisis de vulnerabilidades en sistemas críticos (SAST/DAST)	Informes de análisis según procedimiento GT-PR-18	31-dic-2026	OAP	0% → 100%	8.8
5. FORMACIÓN EN SEGURIDAD						
5.1	Publicar plan de comunicaciones en seguridad	Plan publicado en SIG	31-mar-2026	OAP	95% → 100%	6.3
5.2	(OM-04) Capacitaciones técnicas para administradores de sistemas críticos	Registros de capacitaciones	30-nov-2026	OAP, DTH	0% → 100%	6.3
5.3	Sensibilizaciones enfocadas a equipos de desarrollo	Registros de talleres	30-nov-2026	OAP, DTH	0% → 100%	8.28
5.4	Ejercicio teórico de crisis cibernética con directivas	Informe con lecciones aprendidas	30-sep-2026	Despacho, OAP	60% → 100%	5.30
6. GESTIÓN DE TERCEROS Y PROVEEDORES						
6.1	Evaluar riesgos de seguridad de la información de proveedores críticos	Matriz de evaluación de riesgos de proveedores críticos	30-sep-2026	OAP, DAF	0% → 100%	5.19, 5.20
6.2	Incluir cláusulas de seguridad de la información en contratos con proveedores críticos	Plantilla de cláusulas contractuales	30-jun-2026	OAP, DAF	0% → 100%	5.21

		actualizada y aplicada				
6.3	Establecer monitoreo y seguimiento a cumplimiento de requisitos de seguridad por parte de proveedores críticos	Informes trimestrales de monitoreo de proveedores	31-dic-2026	OAP	0% → 100%	5.22

Elaboración Oficina Asesora de Planeación, 2026.

Nuevos Controles ISO 27001:2022 Incorporados

El plan 2026 incorpora actividades alineadas con los **11 nuevos controles** introducidos por ISO 27001:2022:

Tabla 3. *Controles incorporados*

Control	Nombre	Actividad Relacionada
5.7	Inteligencia de amenazas	OM-02 SIEM, OM-04 Formación técnica
5.23	Seguridad de servicios en la nube	Evaluación de expansión SIEM a servicios cloud
5.30	Preparación TIC para continuidad	OM-03 Guías de contingencia, Actualización BIA
8.9	Gestión de la configuración	OM-08 Socialización trazabilidad administradores
8.10	Eliminación de información	OM-05 Socialización política eliminación segura
8.11	Enmascaramiento de datos	OM-06 Socialización política enmascaramiento
8.12	Prevención de fuga de datos	Etiquetado DLP
8.16	Actividades de monitoreo	OM-02 SIEM institucional
8.23	Filtrado web	Incluido en políticas DLP
8.28	Codificación segura	OM-09 Guía desarrollo seguro, Sensibilizaciones

Elaboración Oficina Asesora de Planeación, 2026.

8. Atención a Oportunidades de Mejora - Auditoría MSPI 2025

En atención al Informe Final de Auditoría Interna al MSPI (Radicado 3-2025-004948), que identificó **13 oportunidades de mejora** y **0 incumplimientos**, el presente plan incorpora las acciones correspondientes para fortalecer el Sistema de Gestión de Seguridad de la Información.

Resultados de la Auditoría MSPI 2025

Tabla 4. *Resultados de Auditoria 2025*

Tipo	Cantidad
Oportunidades de Mejora	13

Cumplimientos	20
Fortalezas	5
Incumplimientos	0

Elaboración Oficina Asesora de Planeación, 2026.

Fortalezas Identificadas en la Auditoría

- Seguridad robusta en servicios en la nube
- Alta concienciación en seguridad del personal
- Controles de acceso físico y lógico bien gestionados
- Política institucional de arquitectura aprobada y alineada
- Hoja de ruta estructurada con proyectos, cronogramas y costos

Referencia Normativa

Las acciones definidas cumplen con:

- Resolución MinTIC 02277 de 2025 - MSPI actualizado
- ISO 27001:2022 - Sistema de Gestión de Seguridad de la Información
- Decreto 612 de 2018 - Integración de planes institucionales

Control de cambios

No.	CAMBIOS REALIZADOS
1	Creación del documento.
2	Actualización integral del plan: (a) Alineación con MSPI 2025 (Resolución 02277) e ISO 27001:2022; (b) Incorporación de 7 oportunidades de mejora de Auditoría MSPI con vinculación a riesgos; (c) Inclusión de actividades para nuevos controles ISO 27001:2022; (d) Inclusión de metas específicas por actividad.

Responsables de elaboración, revisión y aprobación

ELABORADO POR	REVISADO POR	APROBADO POR	AVALADO POR
Cristian Camilo Calderón Tapia	Paula Vanessa Sosa Martin	Yurieth Paola Rojas Mayorga	Yurieth Paola Rojas Mayorga
Contratista OAP	Contratista OAP	Jefe Oficina Asesora de Planeación	Jefe Oficina Asesora de Planeación