

Oficina de Control Interno

Secretaría General Alcaldía Mayor de Bogotá D.C.

Auditoría Regular

Modelo de Seguridad y Privacidad de la Información - MSPI

Informe Final

8 de octubre de 2026

**ALCALDÍA MAYOR
DE BOGOTÁ**

	PROCESO	Evaluación del sistema de control interno	CÓDIGO	4201000-FT-1127
	PROCEDIMIENTO	Auditorías internas de gestión	VERSIÓN	02
	FORMATO	Informe de Auditoría interna de Gestión	PÁGINA	1 de 11

Auditoría Especial ☐	Auditoría Regular ☒
--	--

1. OBJETIVO DE LA AUDITORÍA

Realizar una evaluación independiente y emitir conclusiones frente a la gestión de riesgos de seguridad de la información en la Secretaría General de la Alcaldía Mayor de Bogotá.D.C. en el marco del Modelo de Seguridad y Privacidad de la Información – MSPI.

2. ALCANCE

El alcance incluyó la evaluación del Modelo de Seguridad y Privacidad de la Información – MSPI para lo corrido de la vigencia 2026.

3. LIMITACIÓN AL ALCANCE

En el desarrollo del trabajo de aseguramiento **No se presentaron limitaciones en el alcance**, toda vez que la información fue suministrada por los líderes y/o responsables de los procesos evaluados en el alcance de la auditoría.

4. CONFORMACIÓN EQUIPO DE TRABAJO DE AUDITORÍA

- Luz Andrea Jaramillo Acero – Administradora Pública - Jefe Oficina de Control Interno
- Juan Camilo Gonzalez Caicedo – Administrador de Empresas – Auditor

	PROCESO	Evaluación del sistema de control interno	CÓDIGO	4201000-FT-1127
	PROCEDIMIENTO	Auditorías internas de gestión	VERSIÓN	02
	FORMATO	Informe de Auditoría interna de Gestión	PÁGINA	2 de 11

5. CONTEXTO

La información contenida en este numeral corresponde al contexto del MSPI en la Secretaría General de la Alcaldía Mayor de Bogotá D.C., tiene origen en la información suministrada por la entidad a la Oficina de Control Interno y su finalidad es orientar al lector, por lo tanto, el contexto no constituye por sí mismo, conclusiones de auditoría respecto a la información presentada por la OTIC, en especial lo relacionado con el cumplimiento, o no, del estándar NTC ISO/IEC 27001:2022.

Modelo de Seguridad y Privacidad de la Información – MSPI

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC define el Modelo de Seguridad y Privacidad de la Información - MSPI como el habilitador de la Política de Gobierno Digital, articulando el ciclo PHVA para estructurar la ciberseguridad, la protección de infraestructura crítica y la gestión del riesgo en las entidades públicas.

Las cinco fases del modelo inician con el Diagnóstico o Análisis GAP para medir la madurez previa, continúan con la Planificación donde se establece el alcance, la política, los roles y la asignación presupuestal en el PETI, pasan a la Operación con la ejecución de controles, evalúan el desempeño mediante auditorías e indicadores, y culminan en el Mejoramiento Continuo con acciones de remediación.

Fase del MSPI	Componentes y Salidas Principales
Diagnóstico	Autodiagnóstico MSPI, análisis de brechas inicial y determinación del nivel de madurez.
Planificación	Alcance formal, política adoptada por resolución, inventario de activos, matriz de riesgos, declaración de aplicabilidad y PETI.
Operación	Implementación de controles ISO/IEC 27001:2022, sistemas de alerta temprana, monitoreo continuo y gestión de vulnerabilidades.
Evaluación del Desempeño	Auditorías internas, informe de efectividad de controles, revisión por la dirección e indicadores FURAG.
Mejoramiento Continuo	Plan anual de mejora, remediación de no conformidades y actualización del plan estratégico de seguridad.

De acuerdo con los lineamientos de MinTIC, la gestión del riesgo exige proteger la confidencialidad, integridad, disponibilidad y privacidad, evaluando amenazas avanzadas persistentes, entornos en la nube y el marco de la Ley 1581 de 2012.

	PROCESO	Evaluación del sistema de control interno	CÓDIGO	4201000-FT-1127
	PROCEDIMIENTO	Auditorías internas de gestión	VERSIÓN	02
	FORMATO	Informe de Auditoría interna de Gestión	PÁGINA	3 de 11

La estructura de controles adopta los 93 controles del Anexo A de la NTC ISO/IEC 27001:2022, distribuidos en cuatro dominios correspondientes a Controles Organizacionales (A.5), Controles de Personas (A.6), Controles Físicos (A.7) y Controles Tecnológicos (A.8).

Dominio ISO/IEC 27001:2022	N° de Controles
A.5 Organizacionales	37
A.6 Personas	8
A.7 Físicos	14
A.8 Tecnológicos	34
	93

MSPI Secretaría General de la Alcaldía Mayor de Bogotá D.C

La Secretaría General de la Alcaldía Mayor de Bogotá adoptó la Política de Seguridad de la Información y Seguridad Digital mediante la Resolución 373 de 2025, integrando el Plan MSPI vigencia 2026 con la plataforma estratégica institucional y el estándar ISO/IEC 27001:2022. La estructura de gobernanza opera bajo la dirección del Comité Institucional de Gestión y Desempeño reglamentado por la Resolución 485 de 2024, y cuenta con el soporte técnico permanente de la Mesa Técnica de Apoyo en Archivo y Seguridad de la Información.

La evaluación del nivel de madurez, realizada por la entidad, y reportada a la Oficina de Control Interno mediante el Instrumento de evaluación MSPI con corte 30 de junio 2026 (en actualización por transición ISO 27001:2022) la sitúa en la categoría Optimizado, registrando una efectividad promedio del 98% en la aplicación de los controles bajo el estándar ISO/IEC 27001:2022, en tal sentido, la calificación desagregada muestra un 99% en Controles Organizacionales (A.5), un 100% en Controles de Personas (A.6), un 100% en Controles Físicos (A.7) y un 91% en Controles Tecnológicos (A.8), concentrando la brecha operativa en la infraestructura técnica.

Dominio ISO/IEC 27001:2022	Calificación Actual	Calificación Objetivo	Nivel de Madurez
A.5 Controles Organizacionales	99%	100%	Optimizado
A.6 Controles de Personas	100%	100%	Optimizado
A.7 Controles Físicos	100%	100%	Optimizado
A.8 Controles Tecnológicos	91%	100%	Optimizado
Promedio General	98%	100%	Optimizado

La estrategia para la vigencia 2026 enfoca sus acciones en cerrar la brecha del 10% en el dominio tecnológico mediante la implementación del sistema XDR, autenticación multifactor - MFA, controles DMARC - Domain-based Message Authentication Reporting and Conformance, entornos sandbox y pruebas del Plan de Recuperación ante Desastres - DRP en la nube. La gestión se articula con el PETI 2025-2027 y el modelo definido en el Decreto Distrital 472 de 2024, asegurando continuidad operativa y cumplimiento estricto del régimen de protección de datos personales.

	PROCESO	Evaluación del sistema de control interno	CÓDIGO	4201000-FT-1127
	PROCEDIMIENTO	Auditorías internas de gestión	VERSIÓN	02
	FORMATO	Informe de Auditoría interna de Gestión	PÁGINA	4 de 11

Valoración de Riesgos

La matriz de valoración de riesgos de la Secretaría General de la Alcaldía Mayor de Bogotá consolida un total de 532 riesgos evaluados tras la aplicación del esquema de controles institucionales.

Distribución Consolidada del Riesgo Residual

- **Riesgo Bajo (74,8%):** Concentra la mayoría de los eventos evaluados (398 riesgos). Muestra que las salvaguardas y controles vigentes mitigan adecuadamente la mayor parte de las amenazas sobre los activos de información.
- **Riesgo Moderado (23,9%):** Afecta a 1 de cada 4 riesgos consolidados (127 riesgos). Requiere el fortalecimiento y ajuste preventivo de los controles técnicos y organizacionales para evitar su escalamiento.
- **Riesgo Alto (1,3%):** Corresponde a 7 riesgos de nivel alto. Constituyen una amenaza institucional inmediata que exige la formulación, ejecución y seguimiento obligatorio de un plan de tratamiento específico.

Riesgo Residual	%	Cantidad	Tratamiento Estratégico Requerido
Bajo	74,8%	398 riesgos	Mantenimiento y monitoreo continuo de los controles vigentes.
Moderado	23,9%	127 riesgos	Fortalecimiento e intervención de controles para reducir su nivel.
Alto	1,3%	7 riesgos	Plan de tratamiento obligatorio de ejecución inmediata.

Priorización 2026

1. Tratamiento de los 7 Riesgos Altos:

Tienen carácter prioritario y están vinculados a activos de información con niveles de criticidad alta (20% del total de activos) y media (49%). Su intervención está bajo la supervisión directa del Comité Institucional de Gestión y Desempeño.

2. Mitigación de la Zona Moderada:

Para reducir el 23,9% de riesgos moderados, el Plan MSPI 2026 articula proyectos tecnológicos como la implementación de la solución XDR, autenticación MFA, protocolos DMARC/SPF/DKIM y la ejecución del DRP para servicios críticos en la nube.

	PROCESO	Evaluación del sistema de control interno	CÓDIGO	4201000-FT-1127
	PROCEDIMIENTO	Auditorías internas de gestión	VERSIÓN	02
	FORMATO	Informe de Auditoría interna de Gestión	PÁGINA	5 de 11

3. Alineación Normativa:

La gestión y actualización de la matriz se realiza conforme a la Guía metodológica para la gestión de riesgos de seguridad digital de la entidad y las exigencias de la norma NTC ISO/IEC 27001:2022.

Acciones para los 7 riesgos altos

- Formulación e intervención prioritaria de planes de tratamiento para mitigar su nivel de exposición.
- Aprobación, seguimiento y control de las medidas por parte del Comité Institucional de Gestión y Desempeño.
- Actualización continua de la matriz de riesgos de seguridad digital, el inventario de activos y sus respectivos planes de tratamiento por parte de la OTIC entre febrero y diciembre.
- Implementación de controles como MFA, DMARC, SPF, DKIM, aislamiento geográfico, sandbox y monitoreo activo mediante XDR.
- Ejecución técnica del Plan de Recuperación ante Desastres (DRP) en la nube para los servicios tecnológicos priorizados entre marzo y diciembre.

Integración del XDR con el PETI 2025–2027

La adopción de la herramienta XDR (Extended Detection and Response) se articula directamente con el Plan Estratégico de Tecnologías de la Información (PETI 2025–2027) y la Estrategia de Seguridad Digital (Resolución 373 de 2025) mediante los siguientes ejes:

- El PETI incluye la implementación del XDR durante la vigencia 2026 para migrar de una gestión de incidentes "reactiva-controlada" (dependiente del reporte manual del usuario) a un esquema de monitoreo preventivo, correlación avanzada de eventos y detección de amenazas en tiempo real.
- La herramienta forma parte de los proyectos de actualización y aseguramiento de la infraestructura tecnológica liderados por la OTIC de enero a diciembre.
- Complementa la protección perimetral frente a picos de phishing, spoofing e intentos de compromiso de cuentas institucionales identificados en la operación.
- Responde al objetivo del PETI y del MSPI de cerrar las brechas tecnológicas identificadas frente al Anexo A de la NTC ISO/IEC 27001:2022 y proteger servicios en la nube

	PROCESO	Evaluación del sistema de control interno	CÓDIGO	4201000-FT-1127
	PROCEDIMIENTO	Auditorías internas de gestión	VERSIÓN	02
	FORMATO	Informe de Auditoría interna de Gestión	PÁGINA	6 de 11

Brechas por dominios ISO/IEC 27001:2022 identificadas por la entidad (Promedio: 96%)

El diagnóstico, realizado por la entidad mediante la herramienta de autodiagnóstico del MSPI determinó un nivel de madurez Optimizado, alcanzando una efectividad promedio del 96% en los controles aplicados.

- Controles Tecnológicos (Dominio A.8 – Calificación: 90%): Constituye la brecha principal (10%), concentrada en la necesidad de estandarizar la protección de datos, la gestión de configuraciones de seguridad, el enmascaramiento y la prevención de fuga de información.
- Controles Organizacionales (Dominio A.5 – Calificación: 94%): Presenta una brecha del 6%, asociada a la formalización documental, inteligencia de amenazas y gobierno de servicios en la nube.
- Controles de Personas (Dominio A.6 – Calificación: 98%): Registra una brecha del 2% orientada a profundizar los planes de socialización y capacitación.
- Controles Físicos (Dominio A.7 – Calificación: 100%): Cumplimiento total sin brecha identificada.
- Pese a lograr el 100% de cierre de los casos reportados en 2025, la entidad identificó brechas en la detección temprana antes de que el usuario efectúe la notificación.
- Necesidad de llevar a cabo la ejecución y prueba técnica del DRP en entornos de nube para garantizar la continuidad de la operación institucional ante fallas masivas.

	PROCESO	Evaluación del sistema de control interno	CÓDIGO	4201000-FT-1127
	PROCEDIMIENTO	Auditorías internas de gestión	VERSIÓN	02
	FORMATO	Informe de Auditoría interna de Gestión	PÁGINA	7 de 11

6. RESULTADOS DE AUDITORÍA

En ejercicio de las funciones de la Oficina de Control Interno y en especial de los roles liderazgo estratégico, enfoque hacia la prevención y evaluación de la gestión del riesgo, descritos en el Decreto 648 de 2017, a continuación, se presentan las recomendaciones derivadas de la aplicación de las pruebas y procedimientos de auditoría adelantados por la Oficina de Control Interno.

Al respecto es pertinente aclarar que, en el marco de la operación del esquema de líneas de aseguramiento, y teniendo en cuenta que el MSPI está estrechamente ligado al cumplimiento del estándar ISO, las recomendaciones que se presentan a continuación no generan plan de mejoramiento y tienen por objeto que la administración ponga en consideración su adopción en pro del fortalecimiento de la gestión institucional del riesgo y del Modelo de Seguridad y Privacidad de la Información.

- 1. Formalizar la inclusión del responsable de seguridad de la información u Oficial de Seguridad de la Información como miembro permanente del Comité Institucional de Gestión y Desempeño** por cuanto, además de tratarse de un requisito establecido en el numeral 7.2.1 del Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información V.5 (MinTIC, 2025), es el encargado de reportar la gestión de seguridad y privacidad de la información a la alta dirección de la entidad para que se tomen las acciones necesarias.

En tal sentido, es necesario recordar que el artículo 7 de la resolución 373 de 10 de septiembre de 2025 determinó que “La implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) en la Secretaría General de la alcaldía Mayor de Bogotá, se efectuará conforme a los lineamientos y normatividad aplicable emitida por el Ministerio de Tecnologías de Información y Comunicaciones (MinTIC) y la Oficina consejería Distrital de Tecnologías de la Información y las Comunicaciones. Además, será alineado con el estándar internacional ISO/IEC 27001, en su versión vigente.”.

Esta recomendación es especialmente relevante teniendo en cuenta que, para 2026 existen 7 riesgos que tienen carácter prioritario y están vinculados a activos de información con niveles de criticidad alta (20% del total de activos) y media (49%) y su intervención está bajo la supervisión directa del Comité Institucional de Gestión y Desempeño.

- 2. Identificar y determinar las partes interesadas, internas y externas, que puedan influir o verse afectadas por la seguridad y privacidad de la información** en los términos descritos en los numerales 7.1.1 y 7.1.2 del Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información V.5 (MinTIC, 2025).

Lo anterior teniendo en cuenta que la dependencia informó a la OCI que no existe documento específico que dé cuenta del análisis de partes interesadas en seguridad de la información, y

	PROCESO	Evaluación del sistema de control interno	CÓDIGO	4201000-FT-1127
	PROCEDIMIENTO	Auditorías internas de gestión	VERSIÓN	02
	FORMATO	Informe de Auditoría interna de Gestión	PÁGINA	8 de 11

que el producto de este análisis es uno de los elementos clave para la identificación de riesgos, la evaluación de sus potenciales impactos, la identificación de infraestructuras críticas y en general la estructura y operación del modelo.

Pese a que el documento suministrado por la dependencia (4202000_MA_022_V13.pdf Manual del Sistema de Gestión) se refiere en algunos apartados a las partes interesadas, este no da cuenta de la identificación y determinación de partes interesadas, internas y externas, que puedan influir o verse afectadas por la seguridad y privacidad de la información.

- Garantizar la independencia jerárquica del Oficial de Seguridad de la Información fuera de la Oficina de Tecnologías de la Información.** El numeral 7.2.3 del Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información V.5 (MinTIC, 2025) establece la necesidad de designar un responsable del MSPI adscrito a un área estratégica distinta a la de Tecnología para evitar conflictos de interés, otorgándole voz y voto en el Comité Institucional de Gestión y Desempeño junto con voz en el Comité de Control Interno.

En el manual de Políticas y Controles de Seguridad y Privacidad de la Información y Políticas de TI 4204000-MA-031, el Oficial de Seguridad de la Información aparece integrado en la estructura de la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC (...). El monitoreo al Modelo de Seguridad y Privacidad de la Información – MSPI (Sistema de Gestión de Seguridad de la Información – SGSI) de la Secretaría General de la Alcaldía Mayor de Bogotá D.C. se realizará de manera interna y bajo la responsabilidad directa de la Oficina de Tecnología de la Información y Comunicaciones – OTIC a través del Oficial de Seguridad de la Información.

- Asignar la propiedad y responsabilidad directa de los riesgos a los líderes de proceso.** El numeral 7.2.3 del Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información V.5 (MinTIC, 2025) dispone que los líderes de cada proceso deben gestionar de forma directa los riesgos de seguridad y privacidad de la información correspondientes a sus actividades; Sin embargo, en el documento 4204000-MA-031 la matriz RACI le otorga al Oficial de Seguridad de la Información y a la OTIC el rol de responsables principales de la identificación y gestión del riesgo, dejando a los dueños de proceso en condición de consultados e informados. En tal sentido, se recomienda actualizar el manual 4204000-MA-031 para definir a los líderes de proceso como aprobadores y responsables directos del análisis y tratamiento de sus riesgos, delimitando el papel del Oficial de Seguridad a la asesoría metodológica y al monitoreo del sistema.
- Evaluar los riesgos de seguridad en la fase precontractual y en el diseño inicial de proyectos.** Los numerales 7.3.2 y 7.3.3 del Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información V.5 (MinTIC, 2025) y la sección 3.1.11 del documento Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas V.5 (MinTIC, 2025), determinan que la gestión del riesgo debe iniciar en la planificación del proyecto e integrarse a las especificaciones de contratación con terceros.

	PROCESO	Evaluación del sistema de control interno	CÓDIGO	4201000-FT-1127
	PROCEDIMIENTO	Auditorías internas de gestión	VERSIÓN	02
	FORMATO	Informe de Auditoría interna de Gestión	PÁGINA	9 de 11

En el manual 4204000-MA-031, los controles de seguridad sobre proveedores y nuevos sistemas concentran la validación en pruebas previas al despliegue en producción lideradas por la OTIC. En tal sentido es pertinente resaltar que trasladar la revisión al final del ciclo de vida eleva los costos de remediación y expone la operación a vulnerabilidades no detectadas a tiempo.

- 6. Formalizar un protocolo de reporte periódico e inmediato de riesgos residuales críticos hacia la alta dirección.** El documento Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas V.5 (MinTIC, 2025) y el numeral 7.2.3 del Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información V.5 (MinTIC, 2025) señalan que el responsable de seguridad digital debe informar a la alta dirección sobre las variaciones en riesgos críticos, vulnerabilidades y servicios esenciales.

La normativa interna de la entidad programa el seguimiento a través de reportes semestrales y cuatrimestrales de avance en planes de tratamiento, sin estructurar un canal directo de alerta temprana ante cambios en la severidad del riesgo. Se recomienda reglamentar la entrega de informes ejecutivos periódicos y extraordinarios al Comité Institucional de Gestión y Desempeño, detallando activos afectados, fluctuaciones del riesgo residual y acciones de mitigación inmediata.

- 7. Integrar metodologías de evaluación para amenazas avanzadas persistentes, servicios en la nube y cadena de suministro.** La valoración de riesgos según el numeral 7.3.2 del Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información V.5 (MinTIC, 2025) exige metodologías que identifiquen amenazas avanzadas persistentes (APT), vulnerabilidades emergentes y los dominios de la NTC ISO/IEC 27001:2022 sobre servicios cloud y proveedores.

Aun cuando la Guía metodológica para la gestión de riesgos de seguridad digital 4204000-GS-096 contempla criterios de frecuencia, impacto reputacional e inoculaciones de inteligencia artificial, omite escalas específicas para calcular la dependencia técnica de terceros e infraestructuras en la nube.

- 8. Fortalecer el Plan Institucional de capacitación garantizando que se incluya al personal técnico de la OTIC** en capacitaciones o trasferencias de conocimientos especializadas en ciberseguridad avanzada para administradores de red, bases de datos y desarrollo, entre otros.

El numeral 7.4.2 de del Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información V.5 (MinTIC, 2025), exige garantizar que las personas cuenten con la formación adecuada para su cargo y fortalecer las competencias de respuesta ante incidentes dirigidos, en tal sentido se recomienda estructurar dentro del Plan Institucional de Capacitación – PIC, módulos técnicos especializados dirigidos al personal técnico de la OTIC para transferir conocimientos en la mitigación de vulnerabilidades.

	PROCESO	Evaluación del sistema de control interno	CÓDIGO	4201000-FT-1127
	PROCEDIMIENTO	Auditorías internas de gestión	VERSIÓN	02
	FORMATO	Informe de Auditoría interna de Gestión	PÁGINA	10 de 11

Teniendo en cuenta que en la prestación de los servicios de soporte TI participan personas que no tienen vinculación laboral con la Secretaría General de la Alcaldía Mayor de Bogotá D.C. se recomienda diseñar espacios de socialización que fortalezcan las capacidades técnicas de los proveedores para dar respuesta a las necesidades específicas que tiene la entidad en asuntos de seguridad de la información.

9. **Establecer escenarios de reevaluación obligatoria de riesgos ante incidentes y cambios significativos.** El numeral 8.2 de Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información V.5 (MinTIC, 2025) y el numeral 3.3.2 del documento Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas V.5 (MinTIC, 2025) establecen la necesidad de efectuar evaluaciones de riesgos a intervalos planificados o de manera inmediata ante la ocurrencia de incidentes de seguridad o cambios organizacionales y tecnológico, a su vez, en el manual de Políticas y Controles de Seguridad y Privacidad de la Información y Políticas de TI 4204000_MA_031_V08., el seguimiento del riesgo se encuentra programado bajo revisiones periódicas sin que se contemple la existencia de eventos que requieran la actualización obligatoria. En tal sentido se recomienda diseñar un protocolo de revisión extraordinaria que exija reevaluar la matriz de riesgos e inventario de activos inmediatamente después de materializarse un incidente crítico o modificarse la infraestructura de TI.

Luz Andrea Jaramillo Acero
 Jefe Oficina de Control Interno
 Secretaría General | Alcaldía Mayor de Bogotá D.C.