MEMORANDO	
Código Depend.:	**2310300**
Para:	**MAURICIO ALEJANDRO MONCAYO VALENCIA DESPACHO DE LA SECRETARIA JURIDICA DISTRITAL**
De:	**OFICINA DE CONTROL INTERNO**
Asunto:	**INFORME FINAL DE AUDITORIA IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN MSPI - 2025**

Referenciado(s)	N/A

Respetado Doctor Moncayo:

En cumplimiento del Plan Anual de Auditoría de la vigencia 2025, me permito remitir el informe final de Auditoría interna a la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI en la Secretaría Jurídica Distrital.

Este informe se da a conocer al señor Secretario y a los miembros del Comité Institucional de Coordinación de Control Interno, en cumplimiento de lo dispuesto en el Decreto 648 de 2017 – Artículo 16. "*Adiciónese al Capítulo 4 del Título 21, Parte 2, Libro 2 del Decreto 1083 de 2015, los siguientes artículos: (…) Parágrafo 1. Los informes de auditoría, seguimientos y evaluaciones tendrán como destinatario principal al representante legal de la entidad y al Comité de Coordinación de Control Interno y/o comité de auditoría y/o junta directiva, y deberán ser remitidos al nominador cuando éste lo requiera*".

Las conclusiones de la auditoría fueron socializadas a la Oficina de Tecnologías de la Información y las Comunicaciones en reunión de cierre realizada el 30 de octubre de 2025, de conformidad con el procedimiento "*Auditoría interna - 2310300-PR031*". Derivado de esto, se surtió la fase de remisión de informe preliminar y retroalimentación del auditado. Ante lo respondido por el proceso, se anexa respuesta del análisis realizado por esta Oficina.

Finalmente, en atención al desarrollo de la auditoría realizada, se copia el informe correspondiente a la dependencia auditada, informando que se identificó una (1) no conformidad durante el ejercicio auditor, por tanto, se requiere formulación de plan de mejoramiento de acuerdo con el procedimiento "*Asesoría, Seguimiento y Evaluación de*

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Planes de Mejoramiento - 2310300- PR-032". Así mismo, se reitera al proceso evaluado, que pueden requerir asesoría a la Oficina de Control Interno para la formulación del plan de mejoramiento.

Atentamente,

OLGA MILENA CORZO ESTEPA

c.c.e.: OSCAR JAVIER SUAREZ RAMOS-OFICINA DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES MARIA PAULA RUEDA MANTILLA-SUBSECRETARIA JURIDICA DISTRITAL MARIA FERNANDA QUIJANO VASQUEZ-DIRECCION DE GESTION CORPORATIVA GERMAN ALBERTO PULIDO PULIDO-OFICINA ASESORA DE PLANEACION
Anexo: N/A
Anexos Digitales: 3

Proyectó: DIEGO ALEXANDER URAZAN FRANCO-OFICINA DE CONTROL INTERNO
Revisó: DIEGO ALEXANDER URAZAN FRANCO-OFICINA DE CONTROL INTERNO |
Aprobó: OLGA MILENA CORZO ESTEPA-OFICINA DE CONTROL INTERNO

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

AUDITORÍA INTERNA
MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - MSPI - ISO 27001

Octubre de 2025

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA JURÍDICA DISTRITAL

TABLA DE CONTENIDO

1. DATOS GENERALES 3
2. OBJETIVO 3
3. ALCANCE 3
4. CRITERIOS 3
5. PROCESO, UNIDAD Y/O ÁREA FUNCIONAL, PROGRAMA, PROYECTO DE INVERSIÓN O SISTEMA DE INFORMACIÓN A AUDITAR: 4
6. PROCEDIMIENTO, SUBUNIDAD Y/O ÁREA FUNCIONAL, SUBPROGRAMA, COMPONENTE Y/O SUBSISTEMA DE INFORMACIÓN A AUDITAR: 4
6.1. METODOLOGÍA 4
6.2. ACTIVIDADES DE AUDITORÍA BASADA EN RIESGOS – ANÁLISIS POR ACTIVIDADES DE CONTROL. 4
6.3. DESARROLLO DE LAS ACTIVIDADES DE AUDITORÍA BASADA EN RIESGOS 7
7. FORTALEZAS 59
8. OPORTUNIDAD DE MEJORA 60
9. NO CONFORMIDADES 60
10. RECOMENDACIONES 64
11. CONCLUSIONES 65

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

1. DATOS GENERALES

Fecha: 01 de octubre de 2025
Lugar: Secretaría Jurídica Distrital
Informe N°: 6
Cliente de la Auditoría: Oficina de Tecnologías de la Información y las Comunicaciones.
Líder Auditor: Diego Alexander Urazán Franco

2. OBJETIVO

Evaluar el grado de implementación y mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI) en la entidad, verificando su alineación con las actualizaciones de la normatividad asociada, enfocándose en garantizar la protección de la información, la gestión integral de riesgos asociados a la seguridad y privacidad en el marco de la Política de Gobierno Digital.

3. ALCANCE

El alcance comprende la verificación de la gestión realizada para la implementación del MSPI en la entidad, cubriendo el periodo de 31 de octubre de 2024 a 30 de septiembre de 2025.

4. CRITERIOS

- ✓ Resolución número 02277 del 2025.
- ✓ Resolución 500 de 2021 – MinTIC - 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 746 de 2022 – MinTIC - Por la cual se fortalece el Modelo de Seguridad y
  Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución número 500 de 2021.
- ✓ Ley 1581 de 2012 - Por la cual se dictan disposiciones generales para la protección de datos personales.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

5. PROCESO, UNIDAD Y/O ÁREA FUNCIONAL, PROGRAMA, PROYECTO DE INVERSIÓN O SISTEMA DE INFORMACIÓN A AUDITAR:

Oficina de Tecnologías de la Información y las Comunicaciones.

6. PROCEDIMIENTO, SUBUNIDAD Y/O ÁREA FUNCIONAL, SUBPROGRAMA, COMPONENTE Y/O SUBSISTEMA DE INFORMACIÓN A AUDITAR:

6.1. METODOLOGÍA

Se realizó la auditoría basada en riesgos de conformidad con la información socializada en la reunión de apertura realizada el día 6 de octubre de 2025.

Para el logro de las actividades de auditoría, se realizaron las siguientes actividades:

- Revisión y cotejo documental.
- Entrevistas con el personal responsable.

6.2. ACTIVIDADES DE AUDITORÍA BASADA EN RIESGOS – ANÁLISIS POR ACTIVIDADES DE CONTROL.

Durante la vigencia 2025, el equipo auditor de la Oficina de Control Interno desarrolló la evaluación al Modelo de Seguridad y Privacidad de la Información – MSPI, en el marco de las disposiciones actualizadas por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, particularmente lo establecido en la Resolución 2277 de 2025 (entrando en vigencia el 3 de junio de 2024), la cual actualiza el Anexo 1 de la Resolución 500 de 2021 y fortalece los lineamientos asociados a la gestión de la seguridad digital y la protección de la información. Para lo anterior, cabe aclarar que

El ejercicio tuvo como propósito verificar la efectividad de la gestión adelantada por la Oficina de Tecnologías de la Información y las Comunicaciones en la implementación y mejora continua del modelo, así como medir el grado de cumplimiento frente a los nuevos requerimientos normativos y técnicos establecidos para las entidades públicas.

La auditoría se orientó a determinar el nivel de madurez institucional del MSPI, revisando la aplicación práctica de lo definido en el Documento Maestro del Modelo de Seguridad y

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Privacidad de la Información versión 5 emitido en la presente vigencia, el cual se subdivide en 5 fases a saber:

1. Diagnóstico.
2. Planificación.
3. Operación.
4. Evaluación del desempeño.
5. Mejoramiento continuo.

Gráficamente el modelo se expresa de la siguiente manera:

Con base en estas fases, el ejercicio auditor estructuró las actividades de control conforme a dicho esquema, de la siguiente manera:

Actividad de control 1 - Diagnóstico:

Dentro del documento maestro para esta fase se describe: *"La fase de diagnóstico permite a las entidades establecer el estado actual de la implementación de la seguridad y privacidad de la información, para tal fin se debe realizar un "Diagnóstico" utilizando el "instrumento de evaluación MSPI" con el que se identifica de forma específica los controles*

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

implementados, se mide el nivel de madurez de la implementación del modelo de seguridad y privacidad de la información y se obtienen insumos fundamentales para la fase de planificación.

Este autodiagnóstico se debe realizar antes de iniciar la fase de planificación y actualizar la información tras terminar la fase de evaluación de desempeño, para identificar los cambios en el nivel de madurez de la implementación del Modelo en la entidad, el resultado que se obtenga después de la fase de evaluación de desempeño se incluirá como un insumo, en la fase de mejoramiento continuo."

Actividad de Control 2 – Planificación:

El documento maestro para esta fase indica: "*Para el desarrollo de esta fase se deben utilizar los resultados de la fase anterior y proceder a elaborar el Plan de Seguridad y Privacidad de la Información, con el objetivo de que la entidad realice la planeación del tiempo, recursos y presupuesto de las actividades que va a desarrollar relacionadas con el MSPI:*".

Actividad de Control 3 – Operación:

Para esta fase el documento maestro MSPI indica: *"Tras finalizar la fase 7 de planeación del MSPI, se iniciará la implementación de los procesos de seguridad de la información: gestión de activos, riesgos, incidentes, vulnerabilidades, tratamiento y evaluación de controles. Se fomentará la cultura de seguridad y se definirán criterios de cumplimiento y mecanismos de control para procesos y servicios externos relevantes, asegurando su alineación con el SGSI."*

Actividad de Control 4 – Evaluación del desempeño:

Validación de la fase de evaluación del desempeño del Modelo de Seguridad y Privacidad de la Información, enfocada en verificar la efectividad de las acciones implementadas durante la fase de operación, mediante el análisis de los indicadores definidos en la etapa de implementación

Actividad de Control 5 – Mejoramiento continuo:

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Validar las actividades adelantadas respecto al plan de mejoramiento continuo de seguridad y privacidad de la información el cual hace parte del modelo.

6.3. DESARROLLO DE LAS ACTIVIDADES DE AUDITORÍA BASADA EN RIESGOS

A continuación se presentan las validaciones realizadas por actividad de control así:

Actividad de control 1 - Diagnóstico:

El documento maestro indica para esta fase como lineamiento; "*Identificar a través de la herramienta de autodiagnóstico (instrumento de evaluación MSPI) el estado actual de la entidad respecto a la Seguridad y Privacidad de la Información.*" Ante esto, y con base en validación realizada con la OTIC, el instrumento actualizado presenta los siguientes datos:

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	Nivel de Madurez
A.5	CONTROLES ORGANIZACIONALES	37	100	REPETIBLE
A.6	CONTROLES DE PERSONAS	48	100	EFECTIVO
A.7	CONTROLES FÍSICOS	53	100	EFECTIVO
A.8	CONTROLES TECNOLÓGICOS	28	100	REPETIBLE
PROMEDIO EVALUACIÓN DE CONTROLES		42	100	EFECTIVO

De acuerdo con los resultados obtenidos en la evaluación de efectividad de controles del Modelo de Seguridad y Privacidad de la Información – MSPI, la entidad presenta un nivel de madurez global "Gestionado", con una calificación promedio del 42 frente a una meta de cumplimiento del 100%. Este resultado refleja una gestión activa y sostenida en la implementación de controles, aunque con oportunidades de fortalecimiento en algunos dominios clave.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

En el análisis por dominio, se evidencia que los controles organizacionales (37%) y los controles Tecnológicos (28%) mantienen un desempeño catalogado como efectivo, lo que indica que los lineamientos, procedimientos y medidas técnicas están implementados, pero requieren actualización y fortalecimiento continuo.

Por su parte, los controles de personas (48%) y los controles físicos (53%) se ubican en nivel gestionado, mostrando avances importantes en la cultura de seguridad, la formación del personal y la protección de los activos físicos de información.

En comparación con la vigencia anterior, donde la evaluación general alcanzó un 80% de cumplimiento, se observa una disminución porcentual en la calificación, atribuible principalmente a la actualización normativa y técnica introducida por la Resolución 2277 de 2025 y la adopción de la ISO27001:2022, así como también a un ejercicio detallado de evaluación y validación por parte de la OTIC.

Dicha actualización redujo los dominios de evaluación de 14 a 4, lo que modificó la ponderación de los controles. Por tanto, aunque el promedio disminuye, esta variación responde a un ajuste metodológico más riguroso y no necesariamente a una pérdida de madurez institucional.

Ahora bien, respecto al avance de cláusulas del modelo de operación (PHVA)

AÑO	COMPONENTE (PHVA)	CLAUSULAS	% de Avance Actual	% Avance Esperado
2025	**Planificación**	Contexto de la organización	8%	14%
		Liderazgo	7%	14%
		Planificación	6%	14%
		Soporte	7%	14%
	Implementación	Operación	6%	16%
	Evaluación de Desempeño	Evaluación del	7%	14%
	Mejora Continua	Mejora	6%	14%
TOTAL			**47%**	**100%**

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Durante la vigencia 2025, se observa un avance en la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, pasando de un 23% de avance en 2024 a un 47% en 2025, lo que refleja una mejora en la gestión y consolidación del modelo. Como se indicó, este progreso se da en el marco de la actualización normativa sobre la cual se redefinieron los criterios y dominios de evaluación, aumentando el nivel de exigencia. Los resultados reflejan una gestión en consolidación, con avances evidentes en planificación, ejecución y mejora continua, aunque persiste la necesidad de seguir fortaleciendo la medición, la documentación de evidencias y la articulación institucional para garantizar la sostenibilidad y efectividad del MSPI.

El instrumento del modelo, al igual que en su versión anterior, contempla un levantamiento de información conformado por 42 ítems. En esta vigencia se procedió a validar principalmente aquellos aspectos que fueron objeto de pronunciamiento por parte de la Oficina de Control Interno durante la auditoría de 2024, obteniéndose los siguientes resultados:

N°	Lista de información a solicitar	Comentario OCI 2024	Seguimiento 2025	Nivel de cumplimiento
1	Tipo de entidad (Nacional, Territorial y categoría)	Entidad De Orden Territorial del Distrito Capital	Sin cambios.	Cumple
2	Misión	misión, visión, funciones y deberes publicados en la página web de la Secretaría Jurídica Distrital en la sección de transparencia (https://secretariajuridica.gov.co/transparencia/mision-vision-funciones-y-deberes)	Sin cambios.	Cumple
3	Análisis de contexto: La entidad debe determinar los aspectos externos e internos que son necesarios para cumplir su propósito y que afectan su capacidad para lograr los resultados previstos en el MSPI.	Como soporte de este aspecto el proceso remite el vínculo al Manual del Sistema Integrado de Gestión CÓDIGO: 2310100-MA-001 versión 06, el cual describe el eje de seguridad de la información con la siguiente definición : "Determinar los lineamientos que permitan proteger la Información y los datos personales que adopta la Secretaría Jurídica Distrital, a través de acciones de aseguramiento de la Información teniendo en cuenta los requisitos legales, operativos, tecnológicos, de seguridad y de la entidad alineados con el contexto de direccionamiento estratégico y de gestión del riesgo con el fin de asegurar el cumplimiento de la integridad, disponibilidad, legalidad y confidencialidad de la información.". Con lo informado, y enfatizando lo descrito por la guía: " La entidad debe determinar los aspectos externos e internos que son necesarios para cumplir su propósito y que afectan su capacidad para lograr los resultados previstos en el MSPI.", no se ha creado documento que describa detalladamente los aspectos para cumplir con el propósito y los temas que podrían afectar la obtención de resultados del MSPI		Cumple
4	Mapa de Procesos	Se evidencia mapas y cartas descriptivas de los procesos publicados en la sección de transparencia de la página web de la Secretaría Jurídica Distrital	Sin cambios.	Cumple

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

N°	Lista de información a solicitar	Comentario OCI 2024	Seguimiento 2025	Nivel de cumplimiento
		(https://secretariajuridica.gov.co/transparencia/informacion-entidad/mapas-cartas-descriptivas)		
5	Organigrama de la entidad, detallando el área de seguridad de la información o quien haga sus veces	Se observa organigrama de la entidad (https://secretariajuridica.gov.co/transparencia/informacion-entidad/estructura-organica), sin embargo, no se detalla el área de seguridad de la información.	Sin cambios.	Cumple
6	Políticas de seguridad de la información formalizada y firmada	Se evidencia la Política de seguridad de la información formalizada y firmada, en la resolución 174 de 07 septiembre de 2021 y la Guía de Implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC versión 1 con fecha 1/09/2021	Sin cambios.	Cumple
7	Organigrama, roles y responsabilidades de seguridad de la información, asignación del recurso humano y comunicación de roles y responsabilidades.	Se observa dentro de la Guía de Implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC. código: 2310200-GS-013 versión: 01, el numeral 4.2.1.1. titulado Roles Y Responsabilidades, el cual describe las actividades a realizar por parte de cada uno de estos		Cumple
8	Documento con el resultado de la autoevaluación realizada a la Entidad, de la gestión de la seguridad y privacidad de la información e infraestructura de red de comunicaciones (IPv4/IPv6), revisado y aprobado por la alta dirección	Se aporta dentro del instrumento MSPI el documento o evidencia con el resultado de la autoevaluación realizada a la Entidad de gestión de la seguridad y privacidad de la información e infraestructura de red de comunicaciones (IPv4/IPv6), Sin embargo, no se evidencia revisado y aprobado por la alta dirección . Parcial	Sin cambios.	Cumple
9	Documento con el resultado de la herramienta de la encuesta de diagnóstico de seguridad y privacidad de la información, revisado, aprobado y aceptado por la alta dirección	Dentro del instrumento MSPI, los documentos nombrados en la columna "NOMBRE DEL DOCUMENTO ENTREGADO" se relacionan actas de la vigencia 2022, sin la debida actualización a la vigencia 2023 y lo corrido de la vigencia 2024 no cumple	Sin cambios.	Cumple
10	Documento con el resultado de la estratificación de la entidad, aceptado y aprobado por la alta dirección	Se aporta la resolución 174 de 07 de septiembre de 2021, sin embargo, este documento no contiene la relación del nivel de complejidad que puede traer la implementación del MSPI para la entidad. Nivel de cumplimiento no cumple.	En la vigencia 2025 se evidencia que la situación permanece igual a la reportada en la auditoría anterior. Se mantiene como soporte la Resolución 174 del 7 de septiembre de 2021, sin que esta contenga la definición o relación del nivel de complejidad institucional asociado a la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI. Adicionalmente, dentro del instrumento de evaluación del MSPI no se diligencia información que permita identificar o sustentar el avance de este ítem.	No cumple

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

N°	Lista de información a solicitar	Comentario OCI 2024	Seguimiento 2025	Nivel de cumplimiento
11	Objetivo, alcance y límites del MSPI (Modelo de Seguridad y Privacidad de la Información)	Se evidencia la Guía de Implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC. CÓDIGO: 2310200-GS-013 VERSIÓN: 01, donde se describe Objetivo y alcance del MSPI (Modelo de Seguridad y Privacidad de la Información).	Sin cambios.	Cumple
12	Procedimientos de control documental del MSPI	El proceso responsable reporta link que direcciona al aplicativo SMART, sin embargo, dentro de los procedimientos del proceso Gestión TIC, no se evidencia y/o explica detalladamente los procedimientos de control documental del MSPI. Nivel de cumplimiento: Parcialmente	Durante la presente vigencia, la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) manifestó que la situación se mantiene sin cambios respecto al periodo anterior. Se continúa utilizando el enlace al aplicativo SMART como medio de consulta, sin que los procedimientos del proceso de Gestión TIC incluyan de forma explícita el detalle del control documental del MSPI. El nivel de cumplimiento permanece Parcial.	Parcial
13	Metodología de Gestión de riesgos	Se observa link que direcciona al aplicativo SMART, allí, al consultar la documentación existente, se identifica la política de administración de riesgos 2310100-OT-004 versión 4, la cual en el numeral 7.2.3 indica las actividades a desarrollar para los riesgos de seguridad de la información.	Durante el seguimiento se evidenció que la entidad se encuentra en proceso de actualización de la Guía de Gestión de Riesgos, en concordancia con los lineamientos establecidos en la nueva versión del documento emitido por el Departamento Administrativo de la Función Pública (DAFP). De acuerdo con lo informado por la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC), la actualización incorporará de manera explícita los riesgos asociados a la seguridad y privacidad de la información, con el fin de fortalecer la articulación de la metodología institucional de riesgos con el Modelo de Seguridad y Privacidad de la Información (MSPI).	Cumple
14	Riesgos identificados y valorados de acuerdo a la metodología.	En el aplicativo SMART al consultar los riesgos de gestión del proceso gestión TIC, se observan riesgos relacionados con seguridad de la información a saber: Ω Posibilidad de afectación reputacional, por revelación o utilización de manera inadecuada de la información confidencial de la entidad, debido a accesos no autorizados a recursos compartidos. Ω Posibilidad de afectación reputacional, por ausencia de mecanismos de seguridad que facilite el acceso no autorizado mediante ataques internos o externos que genere la pérdida de integridad de la información., debido a problemas de hardware y/o software, acceso no autorizado a la información, perdida de Integridad del catálogo de servicios, pérdida de Confidencialidad de la información que reside en los ACTIVOS. Ω Posibilidad de afectación reputacional en la entidad, por pérdida de disponibilidad de los sistemas de información, debido al inadecuado soporte a la infraestructura tecnológica que incluye: Problemas de hardware y/o software, Acceso no autorizado a la información, Pérdida de Integridad del catálogo de servicios y Pérdida de Confidencialidad. Ω Posibilidad de afectación reputacional, por pérdida de	Durante el seguimiento se evidenció que la entidad se encuentra en proceso de actualización de la Guía de Gestión de Riesgos, en concordancia con los lineamientos establecidos en la nueva versión del documento emitido por el Departamento Administrativo de la Función Pública (DAFP). De acuerdo con lo informado por la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC), la actualización incorporará de manera explícita los riesgos asociados a la seguridad y privacidad de la información, con el fin de fortalecer la articulación de la metodología institucional de riesgos con el Modelo de Seguridad y Privacidad de la Información (MSPI).	Cumple

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

N°	Lista de información a solicitar	Comentario OCI 2024	Seguimiento 2025	Nivel de cumplimiento
		integridad debido al acceso de forma fraudulenta a la información de la entidad, mediante la impericia humana, o alteración de la configuración o sabotaje.		
15	Planes de tratamiento de los riesgos	Se observa link https://secretariajuridica.gov.co/sites/default/files/2022-01/2310200-GS-009%20Gu%C3%ADa%20Tratamiento%20de%20Riesgos%20de%20Seguridad%20de%20la%20Informaci%C3%B3n_copia_controlada.pdf que nos dirige a la Guía Tratamiento de Información de Riesgos de Seguridad de la Información, donde se establecen las actividades para el tratamiento y mitigación de los riesgos identificados para los activos de información; adicionalmente, en SMART dentro de los riesgos de gestión del proceso Gestión TIC mencionados anteriormente, se contemplan los controles asociados	Se evidencia el cumplimiento del requisito mediante la publicación del Plan de Tratamiento de Riesgos de Seguridad de la Información, disponible en el portal institucional de la Secretaría Jurídica Distrital a través del enlace: https://www.secretariajuridica.gov.co/node/4170. El documento se encuentra accesible para consulta pública y contiene los lineamientos y acciones definidos por la entidad para la administración de los riesgos asociados a la seguridad y privacidad de la información, en concordancia con los requerimientos del Modelo de Seguridad y Privacidad de la Información – MSPI y la Política de Administración de Riesgos Institucional.	Cumple
16	Formatos de acuerdos contractuales con empleados y contratistas para establecer responsabilidades de las partes en seguridad de la información	No se aportan evidencias de los Formatos de acuerdos contractuales con empleados y contratistas para establecer responsabilidades de las partes en seguridad de la información, sin embargo en el seguimiento realizado, se observa que la entidad cuenta con el documento 2310200-FT-268 Compromiso de Confidencialidad de Información, por medio del cual se especifican los derechos y deberes de los colaboradores, antes, durante y después del vínculo contractual, de igual se evidenció que dentro de los contratos de prestación de servicios se encuentra inmerso la cláusula 18 titulada CONFIDENCIALIDAD DE LA INFORMACIÓN, la cual describe : "Garantizar la confidencialidad de la información a la cual el contratista tenga acceso o reciba por parte de la entidad, la cual solamente podrá usarse para la ejecución del contrato. Por lo anterior, el contratista se compromete a respetar, reservar, no copiar, no difundir de ninguna manera, los datos, estructuras, know how, entre otros que se manejen durante la ejecución del contrato. De igual forma, en caso de que exista información sujeta a alguna reserva legal, las partes deben mantener la confidencialidad de esta información. Para ello, debe comunicar a la otra parte que la información suministrada tiene el carácter de confidencial".	La OTIC informa que como parte de su obligación contractual, contratistas y terceros aceptan y firman los términos y condiciones del contrato, el cual establece sus obligaciones y las obligaciones de la entidad para la seguridad de información.	Cumple
17	Procedimiento de verificación de antecedentes para candidatos a un empleo en la entidad	Se ha identificado inconsistencia en el acceso al documento 'Vinculación de Servidores Públicos en Cargos de Libre Nombramiento y Remoción', código 2311300-PR-069, versión 04, en el sitio web de la Secretaría Jurídica Distrital. A pesar de que la entidad cuenta con este procedimiento, el enlace proporcionado por la OTIC (http://www.bogotajuridica.gov.co/intranet/sig/2311300-PR-069.pdf) redirigir a una página de error 'no encontrada'. Se recomienda verificar la disponibilidad del documento a través de los canales oficiales. Nivel de cumplimiento: Parcialmente	Sin cambios.	Cumple
18	Documento con el plan de comunicación, sensibilización y capacitación en seguridad de la información, revisado	Se observa link https://smart.bogotajuridica.gov.co/SJD/portal/resultados_busqueda.php, suministrado por la OTIC en el instrumento de medición MSPI, sin embargo, en este link no se puede acceder a este sitio web; adicionalmente, no se aporta dentro de las evidencias el documento con el plan de comunicación,	Durante la vigencia 2025, la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) elaboró el Plan de Capacitación y Estrategia de Divulgación y Sensibilización en Seguridad de la Información, con el propósito de fortalecer la cultura organizacional en torno a la protección de los activos de	Cumple

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

N°	Lista de información a solicitar	Comentario OCI 2024	Seguimiento 2025	Nivel de cumplimiento
	y aprobado por la alta Dirección, con sus respectivos soportes.	sensibilización y capacitación en seguridad de la información, revisado y aprobado por la alta Dirección, con sus respectivos soportes, solicitado por el instrumento MSPI. Nivel de cumplimiento: No Cumple	información y promover el cumplimiento de los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI).	
19	Documento que haga claridad sobre el proceso disciplinario en caso de incumplimiento de las políticas de seguridad de la información	Se observa link https://secretariajuridica.gov.co/sites/default/files/2022-07/2310200-GS-013%20Gu%C3%ADa%20de%20Seguridad%20y%20Privacidad%20de%20la%20Informaci%C3%B3n%20Seguridad%20Digital%20y%20Continuidad%20de%20la%20Operaci%C3%B3n%20de%20los%20servicios%20TIC_copia_controlada-2.pdf donde se observa guía de implementación de la política de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios TIC, en el numeral 4.3.2.3 titulado Proceso Disciplinario se indica que "En caso de que un servidor, proveedores, o partes interesadas incumplan estas políticas por negligencia o intencionalmente, la Entidad se reserva el derecho de tomar las medidas correspondientes, tales como acciones disciplinarias, suspensión, despido, acciones legales, reclamo de compensación por daños u otros. En el caso de que un funcionario se vea involucrado en incumplimiento de estas políticas se aplicará lo establecido en el Código Disciplinario Único. La Dirección Distrital de Asuntos Disciplinarios será la encargada de investigar y de ser necesario iniciar el proceso disciplinario."	Durante el seguimiento realizado, la dependencia remitió el vínculo correspondiente a la **Resolución 174 de 2021**, mediante la cual se adopta la **Política de Seguridad de la Información** de la entidad. En su numeral **4.3.2.3 "Proceso Disciplinario"**, se establece que, en caso de incumplimiento de las políticas de seguridad por parte de servidores públicos, proveedores o partes interesadas, la entidad podrá adoptar las medidas correspondientes, incluyendo acciones disciplinarias, suspensión, despido, acciones legales o reclamaciones por daños, según la gravedad de la falta.	Cumple
20	Inventario de activos de información clasificados, de la entidad, revisado y aprobado por la alta dirección	Se observa link https://secretariajuridica.gov.co/transparencia/7_datos_abiertos?field_datos_abiertos_target_id=118&field_fecha_de_emision_document_value=All donde se evidencia el Inventario de activos de información clasificados, de la entidad publicado en la página web de la Secretaría Jurídica Distrital vigencia 2024. Cumple.	Durante el seguimiento realizado, se verificó que en la página web institucional se encuentra publicado el Registro de Activos de Información correspondiente a la vigencia 2024, en cumplimiento de los lineamientos establecidos por la Política de Seguridad de la Información y las disposiciones del Modelo de Seguridad y Privacidad de la Información – MSPI. Respecto al Registro de Activos de Información de la vigencia 2025, la dependencia informó que el documento se encuentra en trámite de aprobación y pendiente de publicación, por lo cual aún no es posible evidenciar su divulgación oficial en el sitio web.	Cumple
21	Inventario de áreas de procesamiento de información y telecomunicaciones	Se observa enlace que contiene el inventario de activos de la información clasificados: https://secretariajuridica.gov.co/transparencia/7_datos_abiertos?field_datos_abiertos_target_id=118&field_fecha_de_emision_document_value=All, para la vigencia 2024. Nivel de cumplimiento: Cumple,	No se tiene actualizado	Cumple
22	Diagrama de red de alto nivel o arquitectura de TI	Se cuenta con información del Diagrama de red de alto nivel de TI que indica el instrumento MSPI.	No se tiene actualizado	Cumple
23	Inclusión de la seguridad de la información en la gestión de proyectos	Se identifica en el numeral 4.2.1.2. titulado Seguridad de la Información en Gestión de Proyectos de la GUÍA DE IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL Y CONTINUIDAD DE LA OPERACIÓN DE LOS SERVICIOS TIC, en el cual se indica que La Oficina de Tecnologías de Información y las Comunicaciones desarrollará e incorporará en el desarrollo de sus proyectos en la parte concerniente a	Sin cambios frente a la vigencia anterior. No obstante, se observa que dentro del instrumento MSPI no se diligencia información asociada a este ítem, por lo cual se recomienda complementar la información, incorporando la evidencia que sustente el cumplimiento del requisito y su trazabilidad frente al modelo.	Cumple

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

N°	Lista de información a solicitar	Comentario OCI 2024	Seguimiento 2025	Nivel de cumplimiento
		los riesgos asociados al proyecto, incluirá una identificación y evaluación de riesgos de seguridad de la información, para los cuales se deben definir controles de seguridad que aporten a su mitigación. Nivel de cumplimiento: Cumple		
24	Inventario de partes externas o terceros a los que se transfiere información de la entidad.	La OTIC en entrevista de auditoría indica que no se transfiere información a ninguna entidad. - Nivel de cumplimiento: No Cumple	No se reporta información en el instrumento MSPI.	No cumple
25	Formato de acuerdo de transferencia de información	Este numeral está directamente relacionado con el punto N° 24 en el cual y de acuerdo a lo indicado por el instrumento, en caso de existir inventario de partes externas a los que se transfiere información, debe complementarse con el formato, ante lo descrito, en la entidad no se cuenta con el formato de acuerdo de transferencia de información. Nivel de cumplimiento: No Cumple	Durante el seguimiento realizado, la OTIC reporta como evidencia el vínculo en el sistema SMART correspondiente al Formato de Acuerdo de Transferencia de Información; sin embargo, al efectuar la verificación, no se identifica el documento en dicho sistema, por lo cual no es posible validar su existencia ni su aplicación. En consecuencia, la evidencia reportada no resulta verificable y el criterio se mantiene pendiente de cumplimiento.	No cumple
26	Inventario de proveedores que tengan acceso a los activos de información, indicando el servicio que prestan o bienes que venden	La entidad no cuenta con el inventario de proveedores con el tipo de acceso que tienen a los activos de información de la entidad. En el instrumento MSPI 2024, la OTIC indica que: "Consulta del listado de proveedores en la plataforma SECOP II", sin detallar lo indicado por el numeral, adicional, nos permitimos indicar que este no es el instrumento requerido por el modelo para garantizar el conocimiento de los terceros que acceden a la información. Nivel de cumplimiento: No Cumple	Durante el seguimiento realizado, la OTIC informó que el Inventario de proveedores con acceso a los activos de información, indicando el servicio que prestan o los bienes que suministran, se encuentra en proceso de construcción.	No cumple.
27	Reporte de eventos e incidentes de seguridad de la información de los últimos 12 meses.	De acuerdo con lo validado con el contratista encargado de la seguridad y privacidad de la información en la OTIC respecto al tema de eventos e incidentes de información, fue manifestado que en los últimos 12 meses (2023-2024) no se han reportado eventos. Adicionalmente, se pregunta al contratista acerca de la base de conocimiento que indica el Manual de Gestión de Incidentes de Seguridad de la Información 2310200-MA-015 en el capítulo titulado objetivo, para hacer trazabilidad del incidente presentado en la vigencia 2022 (ataque a servidor de pruebas), a lo cual fue informado que no se cuenta con la mencionada base de conocimiento pero que se deja registro en SMART en el módulo de SGSI; efectivamente en este sistema, se valida la existencia de 5 registros de incidentes reportados desde la vigencia 2020 Finalmente, informamos que este aspecto se cumple, sin embargo, se insta a validar el método de identificación de eventos o incidentes de seguridad de la información, puesto que se han pasado dos vigencias y el hecho de no tener registros nuevos, se podría incurrir en riesgos. Nivel de cumplimiento: Cumple	El proceso informó que se presentaron 17 eventos de seguridad de la información. Sin embargo, aunque la OTIC presentó un formato para el registro y seguimiento de los incidentes, se evidenció que este no se encuentra oficializado en el Sistema Integrado de Gestión (SIG) de la entidad, situación que debe ser atendida con el fin de garantizar la estandarización y trazabilidad formal de la gestión de incidentes de seguridad de la información.	Cumple
28	Plan de continuidad de la Entidad aprobado	En el sistema integrado de gestión a través del sistema SMART, se tiene publicado para el proceso gestión de TIC el Plan de Continuidad del Negocio código 2310200-PL-019 con fecha de vigencia 29/11/2021. Con esto se atiende a lo solicitado por el MSPI, sin embargo, se recomienda realizar un proceso de validación para actualizar el mencionado plan,	Sin cambios.	Cumple

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA JURÍDICA DISTRITAL

N°	Lista de información a solicitar	Comentario OCI 2024	Seguimiento 2025	Nivel de cumplimiento
		puesto que dentro de este en el numeral 7,2, se indica que : "De manera práctica la información debe ser revisada y actualizada con una periodicidad mínima semestral, con cortes a los meses de abril y octubre de cada año, presentada a la Oficina de Tecnologías de la Información y las comunicaciones dentro de los cinco (5) primeros días hábiles siguientes a dichos cortes, con el fin de formalizar su actualización dentro del Plan de Continuidad del Negocio. Lo anterior sin perjuicio de las actualizaciones que los responsables de los procesos consideren necesarias realizar en cualquier momento y/o cuando se presenten cambios sustanciales en la misma", y de acuerdo a las evidencias aportadas, no se observa los procesos de revisión periódicos. Nivel de cumplimiento: Cumple		
29	Inventario de obligaciones legales, estatutarias, reglamentarias, normativas relacionadas con seguridad de la información	Dentro del Sistema Integrado de Gestión a través del aplicativo SMART, en la sección de normograma, se filtra por el proceso Gestión de TIC, obteniendo el listado de circulares, decretos, directivas y resoluciones directamente relacionadas con seguridad de la información. Por lo descrito, la entidad cumple este aspecto. Nivel de cumplimiento: Cumple	Sin cambios.	Cumple
30	Listado de auditorías relacionadas con seguridad de la información realizadas en la entidad	La Oficina de Control Interno ejecutó un proceso de auditoría al modelo de seguridad y privacidad de la información MSPI en la vigencia 2022. Adicionalmente, respecto a la auditoría informada por la OTIC que fue realizada por la Alta Consejería Distrital de TIC, fue solicitada evidencia de dicha actividad, informando que se encontraban en búsqueda de los soportes relacionados. Nivel de cumplimiento: Cumple	La Oficina de Control Interno (OCI) realizó, al finalizar la vigencia 2024, una auditoría al Modelo de Seguridad y Privacidad de la Información (MSPI), con el fin de evaluar el cumplimiento de los lineamientos institucionales y las disposiciones normativas vigentes en materia de seguridad de la información.	Cumple
31	Procedimientos, manuales, guías, directrices, lineamientos, estándares, instructivos relacionados con seguridad de la información, el modelo de seguridad y privacidad de la información de MinTic y Gobierno Digital	Dentro del Sistema Integrado de Gestión a través del aplicativo SMART, en se filtra por el proceso Gestión de TIC, obteniendo el listado entre otros de los siguientes elementos relacionados con seguridad de la información así: ● 2310200-GS-001 Guía para el Registro y la Clasificación de Activos de Información. ● 2310200-GS-009 Guía Tratamiento de Riesgos de Seguridad de la Información ● 2310200-GS-012 Guía para el Registro del Índice de Información Clasificada y Reservada. ● 2310200-GS-013 Guía de Seguridad y Privacidad de la Información Seguridad Digital y Continuidad de la Operación de los servicios TIC. ● 2310200-MA-014 Manual de la Política de Tratamiento y Protección de Datos Personales. ● 2310200-MA-015 Manual de Gestión de Incidentes de Seguridad de la Información. ● 2310200-PL-003 Plan de contingencia. ● 2310200-PL-012 Plan Estratégico de Seguridad de la Información PESI. ● 2310200-PL-019 Plan de Continuidad del Negocio. ● 2310200-PR-025 Registro de Activos de Información e Índice de Información Clasificada y Reservada.	Adicional a los documentos mencionados en 2024 se suman para la presente vigencia: ● 2310200-PL-021 Programa Integral de Protección de Datos Personales. ● 2310200-PR-091 Administración de Usuarios ● 2310200-PR-101 Gestión de Vulnerabilidades	Cumple

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

N°	Lista de información a solicitar	Comentario OCI 2024	Seguimiento 2025	Nivel de cumplimiento
		• 2310200-PR-132 Gestión de acceso. Nivel de cumplimiento: Cumple		
32	Indicadores y métricas de seguridad de la información definidos.	Dentro del instrumento MSPI remite como soporte el vínculo a la batería de indicadores oficiales de la entidad. Adicionalmente, al validar este tema de acuerdo con los soportes remitidos por la OTIC respecto a indicadores del MSPI, fue evidenciado un indicador titulado "NIVEL DE CUMPLIMIENTO DE IMPLEMENTACION DEL MSPI" relacionado con seguridad de la información. Con lo informado y de acuerdo con el documento Indicadores de Gestión de Seguridad de la Información versión 4 del MSPI, asociado al Manual de Gobierno Digital, indica como objetivo que: "La creación de indicadores de gestión está orientada principalmente en la edición de efectividad, eficiencia y eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información, indicadores que servirán como insumo para el componente de mejora continua, permitiendo adoptar decisiones de mejora", nos permitimos informar y entendiendo la existencia del indicador de nivel de cumplimiento del modelo, la entidad no cuenta con indicadores que apunten a la medición de la gestión en materia de seguridad de la información, por tanto este aspecto no se está cumpliendo. Nivel de cumplimiento: No Cumple	La Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) tiene publicados en el aplicativo SMART los indicadores oficiales del Sistema de Gestión de Seguridad de la Información (SGSI), los cuales permiten medir la eficacia y avance en la gestión de la seguridad y la operación tecnológica institucional. Los indicadores definidos son los siguientes: 1. Nivel de funcionamiento de las herramientas tecnológicas y LegalBog 2. Nivel de cumplimiento de implementación del MSPI 3. Porcentaje de controles de seguridad de la información implementados 4. Porcentaje de disponibilidad de los servicios tecnológicos de la entidad 5. Porcentaje de ejecución del plan de mantenimiento y optimización de las plataformas de hardware y software de la SJD 6. Porcentaje de funcionamiento de los sistemas de información de la entidad 7. Porcentaje de incidentes gestionados relacionados en el marco de la seguridad y privacidad de la información institucional 8. Porcentaje de requerimientos de atención del servicio TIC 9. Porcentaje de satisfacción en la prestación del servicio TIC	Cumple
33	Declaración de aplicabilidad	Se cuenta con la declaración de aplicabilidad la cual se cargó oficialmente en el sistema SMART con 110 controles.	En el sistema SMART se tiene publicada la declaración de aplicabilidad con 110 controles	Cumple
34	Aceptación de los riesgos residuales por parte de los dueños de los riesgos	El vínculo reportado por el proceso responsable en el instrumento MSPI apunta a Mapa de riesgos de gestión 2022-Versión 3, en los cuales se reporta por parte del proceso gestión de TIC riesgos relacionados con seguridad de la información, sobre los cuales y propiamente en la columna tratamiento del riesgo se determina o cataloga si el riesgo es aceptado o se reduce. No obstante, en la sección de transparencia de la página web (4.3.10. Planeación, Presupuesto e Informes/ Segundo monitoreo de riesgos de gestión 2024), se reporta el seguimiento a riesgos vigencia 2024 con las mismas condiciones indicadas, por lo tanto, se cuenta con información actualizada. Nivel de cumplimiento: Cumple	Sin cambios.	Cumple
	Lista de información para aquellas entidades que hayan avanzado en la fase			

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

N°	Lista de información a solicitar	Comentario OCI 2024	Seguimiento 2025	Nivel de cumplimiento
	de IMPLEMENTACIÓN			
35	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	En el link https://secretariajuridica.gov.co/sites/default/files/2022-03/PLAN%20ESTRAT%C3%89GICO%20DE%20SEGURIDAD%20DE%20LA%20INFORMACI%C3%93N%20%20PESI.pdf, se puede evidenciar que la Entidad cuenta con el documento "PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN – PESI" CÓDIGO - 2310200-PL-012 V1. Nivel de cumplimiento: Cumple	Sin cambios.	Cumple
36	Avance en la ejecución del plan de tratamiento de riesgos	En el link citado (https://secretariajuridica.gov.co/node/2671), se puede evidenciar el direccionamiento a la sección de transparencia en la página web de la SJD, observando que se encuentra publicado el "Mapa de riesgos de gestión 2022-Versión 3", con fecha de emisión Lun, 19/09/2022, como también se evidencia la publicación el "Plan Anticorrupción y de Atención al Ciudadano", con fecha de publicación Lun, 19/09/2022. Adicional se observa en la sección de transparencia 4.3.10. Planeación, Presupuesto e Informes/ Segundo monitoreo de riesgos de gestión 2024 link de verificación https://www.secretariajuridica.gov.co/4-planeacion-presupuesto-e-informes?field_4_planeacion_presupuesto_e_target_id=145&field_fecha_de_emision_document_value=11#:~:text=Mapa%20de%20riesgos%20de%20gesti%C3%B3n%202024%20%2D%20Versi%C3%B3n%202. El cual refleja el avance de gestión de los riesgos asociados al proceso de gestión TIC. Nivel de cumplimiento: Cumple	Se evidencia documento actualizado Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, está incluido dentro del Plan Estratégico de Seguridad de la información 2025 en el vinculo https://www.secretariajuridica.gov.co/4-planeacion-presupuesto-e-informes?field_4_planeacion_presupuesto_e_target_id=147&field_fecha_de_emision_document_value=All	Cumple
37	Indicadores de gestión del MSPI definidos, revisados y aprobados por la alta Dirección.	El proceso auditado dentro del instrumento MSPI remite como soporte el vínculo a la batería de indicadores oficiales de la entidad, Adicionalmente, al validar con la OTIC el tema de indicadores del MSPI, fue evidenciado un indicador titulado "NIVEL DE CUMPLIMIENTO DE IMPLEMENTACION DEL MSPI" relacionado con seguridad de la información De acuerdo con lo mencionado, se evidencia la existencia de los indicadores relacionados, pese a ello, el documento Indicadores de Gestión de Seguridad de la Información versión 4 del MSPI, asociado al Manual de Gobierno Digital, indica como objetivo que: "La creación de indicadores de gestión está orientada principalmente en la edición de efectividad, eficiencia y eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información, indicadores que servirán como insumo para el componente de mejora continua, permitiendo adoptar decisiones de mejora", lo reportado por el proceso responsable no apunta a lo requerido propiamente por el instrumento, por tanto, se	La Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) tiene publicados en el aplicativo SMART los indicadores oficiales del Sistema de Gestión de Seguridad de la Información (SGSI), los cuales permiten medir la eficacia y avance en la gestión de la seguridad y la operación tecnológica institucional. Los indicadores definidos son los siguientes: 10. Nivel de funcionamiento de las herramientas tecnológicas y LegalBog 11. Nivel de cumplimiento de implementación del MSPI 12. Porcentaje de controles de seguridad de la información implementados 13. Porcentaje de disponibilidad de los servicios tecnológicos de la entidad 14. Porcentaje de ejecución del plan de mantenimiento y optimización de las plataformas de hardware y software de la SJD 15. Porcentaje de funcionamiento de los sistemas de información de la entidad	Cumple

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

N°	Lista de información a solicitar	Comentario OCI 2024	Seguimiento 2025	Nivel de cumplimiento
		informa el incumplimiento de lo definido en este numeral. Nivel de cumplimiento: No Cumple	16. Porcentaje de incidentes gestionados relacionados en el marco de la seguridad y privacidad de la información institucional 17. Porcentaje de requerimientos de atención del servicio TIC 18. Porcentaje de satisfacción en la prestación del servicio TIC	
	Lista de información para aquellas entidades que hayan avanzado en la fase de EVALUACIÓN DE DESEMPEÑO			
38	Documento con el plan de seguimiento, evaluación, análisis y resultados del MSPI, revisado y aprobado por la alta Dirección.	En el instrumento MSPI 2024 remitido por el proceso evaluado, se describe que: "Se han presentado los avances de la implementación del MSPI en los comités de gestión y desempeño de los meses de marzo, abril, junio y octubre de 2022. Actas de las reuniones en la Oficina Asesora de Planeación". Se observa desactualización de la información incluida en el instrumento MSPI, la cual corresponde a 2022. Sin embargo, se observa que en la presente vigencia, respecto a revisión y monitoreo del Modelo, en el Comité Institucional de Gestión y Desempeño con fecha 7 de junio se trataron temas de Plan Estratégico de Seguridad de la Información y Plan de Tratamiento de Riesgos de Seguridad, de todas formas, se sugiere validar y reforzar el tema de las evidencias documentales, así como la explicación que se registra sobre el instrumento. Nivel de cumplimiento: Cumple	El responsable del modelo en la OTIC informa que no se ha elaborado el documento con el plan de seguimiento, evaluación, análisis y resultados del Modelo de Seguridad y Privacidad de la Información (MSPI), revisado y aprobado por la Alta Dirección;	No cumple
39	Documento con el plan de auditorías internas y resultados, de acuerdo a lo establecido en el plan de auditorías, revisado y aprobado por la alta Dirección.	El proceso auditado informa que: "Se han realizado auditorias de seguridad de seguridad de la información en la entidad desde el 2020: dos realizadas por la Oficina de Control Interno y una por la Alta Consejería Distrital de TIC". La Oficina de Control Interno en la vigencia 2022 realizó seguimiento al avance de la implementación del modelo de seguridad y privacidad de la información en la entidad generando el correspondiente informe, ya para la vigencia 2024 se contrató profesional auditor para la evaluación del modelo nuevamente. En referencia a la auditoría realizada por la Alta Consejería Distrital de TIC, fue solicitada a la OTIC evidencia que soporte dicho ejercicio, sin embargo, no se obtuvo acceso al mencionado registro. Nivel de cumplimiento: Cumple	En el plan anual de auditoría aprobado en la entidad, se encuentra programada para la vigencia 2025 la realización de una auditoría al Modelo de Seguridad y Privacidad de la Información (MSPI), por lo cual este criterio se considera cubierto conforme a la planificación establecida en dicho documento.	Cumple
40	Resultado del seguimiento, evaluación y análisis del plan de tratamiento de riesgos, revisado y aprobado por la alta Dirección.	El enlace suministrado permite observar el reporte de mapa de riesgos 2022, se deben actualizar los enlaces e información que se asocia al documento de autodiagnóstico, puesto que para el 2024 se cuenta con la publicación de los riesgos aprobados actualizados con el correspondiente monitoreo. Nivel de cumplimiento: Cumple	En el vínculo https://www.secretariajuridica.gov.co/4-planeacion-presupuesto-e-informes?field_4_planeacion_presupuesto_e_target_id=147&field_fecha_de_emision_document_value=All se tiene publicado el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, está incluido dentro del Plan Estratégico de Seguridad de la información – 2025.	Cumple
	Lista de información para aquellas entidades que hayan avanzado en la fase de MEJORA CONTINUA			

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

N°	Lista de información a solicitar	Comentario OCI 2024	Seguimiento 2025	Nivel de cumplimiento
41	Documento con el plan de seguimiento, evaluación y análisis para el MSPI, revisado y aprobado por la alta Dirección.	Se evidencia acta del Comité Institucional de Gestión y Desempeño con fecha 7 de junio en el que se trataron temas de Plan Estratégico de Seguridad de la Información y Plan de Tratamiento de Riesgos de Seguridad. Nivel de cumplimiento: Cumple	La OTIC informa que no se ha elaborado el documento con el plan de seguimiento, evaluación, análisis y resultados del Modelo de Seguridad y Privacidad de la Información (MSPI), revisado y aprobado por la Alta Dirección.	No cumple
42	Documento con el consolidado de las auditorías realizadas de acuerdo con el plan de auditorías, revisado y aprobado por la alta dirección y verifique como se asegura que los hallazgos, brechas, debilidades y oportunidades de mejora se subsanen, para asegurar la mejora continua.	La Oficina de Control Interno ha realizado auditoria a la implementación del MSPI en las vigencias 2022 y la que actualmente se encuentra en proceso de ejecución. Estas se encuentran definidas dentro de los planes anuales de auditoría, los cuales se han aprobado por la Alta Dirección en el Comité Institucional de Control Interno. Nivel de cumplimiento: Cumple	La Oficina de Control Interno ha venido dando continuidad a la evaluación del Modelo de Seguridad y Privacidad de la Información (MSPI), mediante la ejecución de auditorías en la vigencia 2024 y la programación de nuevas evaluaciones en el Plan Anual de Auditoría 2025. Estas acciones demuestran la inclusión permanente del modelo dentro del ejercicio de control interno, contribuyendo al seguimiento del cumplimiento, a la identificación de oportunidades de mejora y al fortalecimiento del sistema de gestión de seguridad y privacidad de la información de la entidad.	Cumple

A continuación, se presenta el resultado del seguimiento de los controles de seguridad y privacidad de la información utilizando el instrumento MSPI, con el fin de medir el nivel de madurez del modelo y obtener insumos para planificación y mejora continua.

La evaluación se organiza en cuatro dominios según ISO 27001:2022 Anexo A: **organizacionales, personas, físicos y tecnológicos**. La OCI presenta los resultados por cada dominio, principalmente con lo registrado en el instrumento por el personal responsable de la OTIC encargados de la implementación del modelo así:

Dominio controles organizacionales:

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
AD.1.1	A 5.1	Políticas de seguridad de la información	60	La entidad cuenta con la Política de Seguridad de la Información debidamente aprobada y publicada.	Se recomienda revisar la calificación asignada, considerando que, aunque existe cumplimiento formal, se reporta una brecha por parte de la OTIC asociada al seguimiento y verificación de su implementación operativa.
AD.1.2	A 5.2	Roles y responsabilidades de	40	De acuerdo con lo establecido en el numeral 7.2.3 de la Guía,	Se encuentra pendiente la definición del Oficial de

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
		seguridad de la información		sobre roles y responsabilidades, la entidad debe designar formalmente un responsable del MSPI con un equipo de apoyo dependiente de un área estratégica distinta a la de Tecnología.	Seguridad de la Información, asunto que actualmente se está gestionando mediante un plan de mejoramiento.
AD.1.3	A 5.3	Segregación de funciones	20	Los sistemas de información institucionales cuentan con roles definidos; sin embargo, la documentación no detalla adecuadamente los mecanismos de segregación de funciones conforme al criterio establecido.	Se recomienda fortalecer la documentación y evidencias que soporten la asignación y control de roles de acceso diferenciados.
AD.1.4	A 5.4	Responsabilidades de la dirección	40	La entidad dispone de una Política de Seguridad de la Información oficializada; no obstante, el componente de roles sigue pendiente por definir, situación reportada desde la vigencia 2024. Se resalta que la alta dirección, a través del Comité Institucional de Gestión y Desempeño, conoce la situación.	Se recomienda continuar con las actividades adelantadas para la definición y actualización de roles y responsabilidades.
AD.1.5	A 5.5	Contacto con las autoridades	60	La Guía de Seguridad y Privacidad de la Información establece la necesidad de mantener contacto con entidades especializadas (MinTIC, ColCERT, CSIRT, Centro Cibernético de la Policía Nacional). Sin embargo, no se definen responsables ni procedimientos específicos para dicha coordinación.	Se recomienda complementar la documentación estableciendo mecanismos y responsables de reporte ante incidentes de seguridad.
AD.1.6	A 5.6	Contacto con grupos de interés especial	60	Como se indicó en el punto anterior, la guía menciona el contacto con grupos de interés, pero no diferencia los canales de comunicación con autoridades competentes.	Se sugiere actualizar los procedimientos y documentación, estableciendo esta distinción para fortalecer la gestión de incidentes y relaciones institucionales.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
AD.1.7	A 5.7	Inteligencia de amenazas	0	En relación con el control de inteligencia de amenazas, orientado a generar conciencia sobre los riesgos emergentes y permitir la adopción de medidas preventivas, la entidad reporta una calificación de 0, ante esto, se enfatiza en desarrollar las actividades requeridas para implementar este control y generar evidencias que soporten su avance.	
AD.1.8	A 5.8	Seguridad de la información en la gestión de proyectos	20	Según el numeral 4.2.1.2 de la Guía, sobre seguridad en la gestión de proyectos, la OTIC debe incorporar la identificación y evaluación de riesgos de seguridad en los desarrollos tecnológicos. Aunque el lineamiento está documentado, no se evidencian soportes en el repositorio de proyectos validado en relación a este tema.	Se recomienda incluir la valoración de riesgos de seguridad de la información en los proyectos que se estén adelantando.
AD.1.9	A 5.9	Inventario de información y otros activos asociados	40	Se verificó la publicación del inventario de activos de información para la vigencia 2024 en la página institucional. La OTIC informa que el inventario de 2025 se encuentra consolidado, aunque aún no se ha publicado, ni verificado.	Se recomienda culminar el proceso de validación y divulgación para asegurar la actualización y disponibilidad de la información
AD.1.10	A 5.10	Uso aceptable de la información y otros activos asociados	40	La Guía de Seguridad y Privacidad de la Información, numeral 4.4.1.3, define la política de uso aceptable de los activos y responsabilidades de los usuarios. No obstante, no se evidencian lineamientos sobre comportamientos esperados, uso permitido o prohibido y actividades de seguimiento.	Se recomienda fortalecer este componente conforme a la documentación de MINTIC y mantener evidencias de su aplicación.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
AD.1.11	A 5.11	Devolución de Activos	40	El numeral 4.4.1.4 de la Guía de Seguridad y Privacidad de la Información establece que los activos asignados deben ser devueltos al finalizar la relación contractual o por cambios en las funciones. Aunque el procedimiento general está descrito, no se evidencia la definición específica para casos de uso de equipos personales o transferencia segura de información institucional	Se recomienda complementar la documentación del proceso con lineamientos que incluyan la trazabilidad y eliminación segura de la información.
AD.1.12	A 5.12	Clasificación de la información	40	Se evidencia la publicación del registro de activos de información, clasificados conforme a tipologías institucionales. No obstante, se observa que el procedimiento de clasificación no cuenta con mecanismos actualizados de revisión o control..	Se sugiere realizar un ajuste documental que contemple puntos de control y actualización periódica conforme a la Guía de Seguridad y Privacidad de la Información
AD.1.13	A 5.13	Etiquetado de la información	40	El numeral 4.4.2.2 de la Guía contempla el etiquetado de la información de acuerdo con su nivel de clasificación. Sin embargo, no se identifican procedimientos detallados que orienten al personal en la aplicación práctica de esta directriz.	Se recomienda incorporar en los procedimientos de la entidad una instrucción operativa que defina responsabilidades, pasos y controles asociados al etiquetado institucional.
AD.1.14	A 5.14	Transferencia de información	40	No se evidencia en la documentación de gestión TIC ni en el sistema SMART un procedimiento formal para la transferencia de información entre dependencias o hacia terceros.	Se sugiere incluir este aspecto dentro de la Guía y los procedimientos relacionados, a fin de garantizar la trazabilidad, confidencialidad y seguridad en las transferencias. En este sentido se recomienda revisar la valoración que se está realizando por parte de la OTIC al referido control.
AD.1.15	A 5.15	Control de acceso	40	El proceso cuenta con un procedimiento formal de gestión de accesos y con políticas de control definidas. No obstante, la OTIC reporta una calificación de 40 al no haberse actualizado los	Se recomienda alinear las actividades con el criterio establecido y documentar las acciones de revisión técnica y administrativa correspondientes.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
				manuales ni las evidencias de segregación de funciones o restricciones de acceso privilegiado.	
AD.1.16	A 5.16	Gestión de la identidad	40	La entidad dispone de un procedimiento de administración de usuarios y políticas complementarias sobre contraseñas y restricciones de acceso. Sin embargo, la calificación de 40 refleja la necesidad de fortalecer la validación del nivel de madurez alcanzado. Durante la auditoría se identificaron debilidades en la administración de usuarios y roles. En la verificación del listado de usuarios activos en el módulo PERNO, se observó que continúan registrados usuarios con roles asociados al módulo de nómina que no pertenecen al proceso funcional responsable (Talento Humano), a pesar de las acciones de depuración realizadas en la vigencia anterior. Esta situación evidencia que las medidas implementadas no han sido eficaces para garantizar el control sostenido sobre los accesos, ni se cuenta con mecanismos de revisión periódica y validación conjunta entre la OTIC y el área funcional, que aseguren la integridad de los usuarios y perfiles asignados. De manera complementaria, se estableció que en el último año no se han efectuado revisiones formales por parte del Oficial de Seguridad de la Información	Se recomienda diagnosticar y revisar los mecanismos de control, actualizar registros de usuarios, documentar y diligenciar el instrumento de acuerdo a lo identificado y avanzado en referencia al tema para todos los sistemas de información de la entidad.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
				sobre los usuarios y roles asignados en el módulo PERNO, conforme a lo establecido en el numeral 4.5.1.1 "Política de Control de Acceso".	
AD.1.17	A 5.17	Información de autenticación	40	El procedimiento de gestión de acceso contempla la autenticación de usuarios, aunque no se encuentran definidos los mecanismos diferenciados aplicables a sistemas con particularidades técnicas.	Se recomienda estandarizar el modelo de autenticación y aplicar controles de robustez acordes con los riesgos identificados en cada plataforma o sistema de información.
AD.1.18	A 5.18	Derechos de acceso	40	A pesar de existir procedimientos generales de gestión de acceso, las auditorías previas evidencian debilidades en la obtención de autorizaciones, segregación de funciones y retiro oportuno de privilegios. Lo anterior se complementar	Se recomienda fortalecer los controles sobre bajas de usuarios, definir un flujo de autorización claro y establecer verificaciones periódicas que aseguren la eliminación efectiva de derechos de acceso.
AD.1.19	A 5.19	Seguridad de la información en las relaciones con proveedores	40	El numeral 4.11 de la Guía contempla las directrices sobre acuerdos de seguridad con terceros.	Si bien la entidad reporta una calificación de 40, no se evidencian soportes documentales que demuestren el cumplimiento de los compromisos de seguridad pactados en los contratos. Para esto, resulta oportuno realizar seguimiento al cumplimiento de este aspecto.
AD.1.20	A 5.20	Abordar la seguridad de la información en los acuerdos con proveedores	40	La OTIC reporta una calificación de 40 sin reportar evidencias de cómo se gestionan los aspectos de seguridad de la información en los procesos contractuales. Se recomienda realizar un diagnóstico y análisis del tema para establecer el grado de cumplimiento y en caso de identificar aspectos a mejorar, generar las acciones articuladamente con las dependencias relacionadas.	No hay evidencias del control, se recomienda revisar la valoración asignada y establecer las actividades necesarias para su formalización.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
AD.1.21	A 5.21	Gestión de la seguridad de la información en la cadena de suministro de las TIC	40	La OTIC reporta una calificación de 40 puntos. No obstante, en la documentación del sistema SMART no se evidencian elementos que acrediten la gestión de la seguridad de la información en la cadena de suministro TIC.	Se recomienda incluir dentro del proceso de gestión TIC, los lineamientos específicos que contemple los controles de seguridad aplicables a proveedores, tal como lo dispone el numeral correspondiente de la Guía de Seguridad y Privacidad de la Información.
AD.1.22	A 5.22	Seguimiento, Revisión y Gestión de Cambios de Servicios de Proveedores	40	Aunque la OTIC señala que revisa los acuerdos de niveles de servicio y los estudios previos de contratación, no se identifican en la guía institucional las actividades formales de seguimiento, revisión y gestión de cambios de servicio con proveedores.	Se sugiere incorporar este aspecto en la documentación del proceso de gestión TIC, a fin de fortalecer la trazabilidad y elevar la calificación otorgada.
AD.1.23	A 5.23	Seguridad de la información para el uso de servicios en la nube	20	El proceso asigna una calificación de 20 puntos, indicando la ausencia de lineamientos sobre seguridad de la información en el uso de servicios en la nube.	Se considera pertinente establecer políticas y procedimientos que regulen el uso de estos servicios, definiendo controles de seguridad, gestión de acceso y custodia de información institucional alojada en entornos externos, lo anterior teniendo en cuenta la implementación de nube pública que actualmente está realizando al OTIC
AD.1.24	A 5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	40	Se cuenta con el Manual de Gestión de Incidentes y la Guía de Seguridad y Privacidad que definen la política institucional.	Con base en la calificación de 40 puntos, se recomienda revisar y actualizar los procedimientos, así como adelantar acciones conforme a los lineamientos del criterio establecido en el instrumento.
AD.1.25	A 5.25	Evaluación y Decisión sobre Eventos de Seguridad de la Información	40	Existen políticas y manuales de gestión de incidentes formalizados en SMART. Sin embargo, se requiere precisar los criterios para categorizar los eventos o incidentes de seguridad de la información.	Se sugiere ajustar la documentación en concordancia los lineamientos asociados a MSPI.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
AD.1.26	A 5.26	Respuesta a los Incidentes de Seguridad de la Información	40	Este numeral se describe en el Manual de Gestión de Incidentes de Seguridad de la Información en SMART, sin embargo la OTIC reporta una calificación de 40, adicional indica que se requiere revisar el procedimiento, así como sensibilizar y preparar a las partes interesadas.	Para este aspecto, se sugiere documentar de forma detallada las actividades a realizar ante un incidente de seguridad de la información, estableciendo entre otros aspectos responsables, tiempos, mecanismos de comunicación y demás información asociada; todo esto asociado a lo descrito en los documentos emitidos por MINTIC.
AD.1.27	A 5.27	Aprendizaje sobre los incidentes de seguridad de la información	40	Si bien el manual menciona la necesidad de cuantificar y monitorear los tipos y costos de los incidentes, no se evidencia la implementación de tales mecanismos.	Se recomienda adelantar acciones de seguimiento que permitan registrar y analizar los incidentes reportados, en cumplimiento de los lineamientos del MSPI.
AD.1.28	A 5.28	Recopilación de pruebas	40	La guía no especifica el proceso para la recopilación de evidencias derivadas de incidentes o eventos de seguridad.	Se recomienda desarrollar las actividades asociadas al manejo de evidencias digitales, garantizando la integridad y trazabilidad conforme a la documentación del modelo y prácticas de la industria.
AD.1.29	A 5.29	Seguridad de la información durante la interrupción	20	La guía institucional no detalla los controles de seguridad aplicables durante interrupciones operativas.	Con base en la calificación de 20 puntos, se sugiere revisar la documentación asociada e incorporar los requisitos específicos de seguridad que deben mantenerse durante dichos eventos.
AD.1.30	A 5.30	Preparación de las TIC para la continuidad del negocio	20	El proceso cuenta con un plan de continuidad institucional y políticas definidas	Se recomienda revisar la documentación existente y evaluar las actividades efectivamente desarrolladas, determinando brechas y pendientes conforme a los . lineamientos del criterio en relación al MSPI.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
AD.1.31	A 5.31	Requisitos legales, estatutarios, reglamentarios y contractuales	40	Se evidencia la identificación de la normatividad aplicable en materia de seguridad de la información, y se adelanta la actualización del instrumento MSPI.	Se recomienda revisar la calificación otorgada y fortalecer las evidencias y la justificación que acrediten el cumplimiento de cada requisito, asegurando la vigencia normativa en los documentos de gestión
AD.1.32	A 5.32	Derechos de propiedad intelectual	40	La Guía de Seguridad y Privacidad incluye lineamientos sobre protección de materiales sujetos a propiedad intelectual.	Con una calificación de 40 puntos, se recomienda actualizar la guía de implementación y fortalecer la gestión documental que evidencie la protección y uso adecuado de estos activos
AD.1.33	A 5.33	Protección de registros	20	La OTIC califica con 20 puntos debido a la falta de detalle sobre los procedimientos para proteger la autenticidad e integridad de los registros.	Se sugiere complementar la guía con actividades específicas de respaldo, conservación y control de accesos, conforme a los criterios del instrumento MSPI
AD.1.34	A 5.34	Privacidad y protección de la PII	20	Sobre el tema en SMART se identifican Manual de la Política de Tratamiento y Protección de Datos Personales, Programa Integral de Protección de Datos Personales y el procedimiento Atención de requerimientos de datos personales.	Con base en la calificación de 20 puntos, se recomienda validar las acciones necesarias y comunicar la política de privacidad institucional, estableciendo roles, responsabilidades y mecanismos de control asociados.
AD.1.35	A 5.35	Revisión independiente de la seguridad de la información	60	Durante las vigencias 2024 y 2025 se realizaron auditorías internas al modelo de seguridad y privacidad.	Se recomienda validar la calificación de 60 puntos y documentar en el instrumento las actividades realizadas.
AD.1.36	A 5.36	Cumplimiento de políticas, normas y estándares de seguridad de la información	40	Si bien se han realizado auditorías internas, no se cuenta con evidencias de revisión directa por parte de la alta dirección o dueños de proceso.	Se sugiere fortalecer la evidencia de revisión directa por estas instancias a fin de garantizar el cumplimiento integral del criterio conforme a lo establecido en los lineamientos del MSPI

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
AD.1.37	A 5.37	Procedimientos operativos documentados	40	La entidad cuenta con lineamientos institucionales y documentación en el SIG que orientan la operación y seguridad de la información.	Se recomienda continuar con las acciones de fortalecimiento documental y operativo, conforme a la calificación de 40 puntos, priorizando la evidencia de cumplimiento y la actualización de los procedimientos

Dominio controles de personas:

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
P.1.1	A 6.1	Revisión de antecedentes	60	En seguimiento a este criterio, la OTIC en el instrumento menciona: se identifica que la entidad cuenta en la Guía de Implementación del MSPI con el numeral 4.3.1 "Selección de personal", el cual establece directrices relacionadas con la revisión de antecedentes y los procesos de selección del talento humano, alineándose con lo dispuesto en este control. Asimismo, se evidencia que los Estudios Previos de Contratación Directa y los Estudios Previos de Otras Modalidades contemplan listas de chequeo mediante las cuales se validan los antecedentes del personal a contratar.	Considerando la calificación otorgada de 60 puntos, la brecha identificada y el hecho de que en el repositorio del modelo no se encuentran soportes que evidencien el cumplimiento total del criterio, por tanto se sugiere adelantar las acciones necesarias para fortalecer y documentar la trazabilidad del cumplimiento, asegurando la disponibilidad de los procedimientos actualizados y sus respectivos registros de verificación.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
P.1.2	A 6.2	Términos y condiciones de empleo	60	En seguimiento a este criterio, se evidencia que la entidad cuenta con lo establecido en la Guía de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios TIC, donde en el numeral 4.3.1.1 "Términos y condiciones laborales" se establece el cumplimiento de los requerimientos de seguridad de la información, indicando además que los funcionarios deben firmar el Acuerdo o Cláusula de Confidencialidad como parte del vínculo contractual.	De acuerdo con la calificación asignada de 60 puntos y la necesidad de asegurar la trazabilidad documental, se recomienda revisar la vigencia y aplicabilidad de los procedimientos asociados, así como garantizar su actualización y el cumplimiento efectivo de las obligaciones contractuales en materia de seguridad de la información, de acuerdo con los lineamientos establecidos en la documentación del MSPI.
P.1.3	A 6.3	Concientización, educación y entrenamiento en seguridad de la información	60	Respecto a este criterio, se evidencia que la entidad cuenta con una estrategia de sensibilización en seguridad de la información, y que en la Guía de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC se encuentra descrita la política sobre toma de conciencia, educación y formación en seguridad de la información.	Dado que no se evidencian en el repositorio soportes documentales que acrediten las capacitaciones realizadas y no se diligenció la brecha correspondiente, se recomienda adelantar las acciones y actividades necesarias relacionadas con la formación y sensibilización del personal, considerando la calificación otorgada de 60 puntos y la relevancia que este aspecto tiene para fortalecer la cultura de seguridad de la información dentro de la entidad
P.1.4	A 6.4	Proceso disciplinario	40	Se identifica que la Guía contempla el numeral 4.3.2.3 sobre el Proceso Disciplinario, el cual establece las acciones aplicables frente al incumplimiento de las políticas de seguridad de la información, haciendo referencia directa al Código Disciplinario Único y designando a la Dirección Distrital de Asuntos Disciplinarios como la instancia responsable de las	En referencia a la calificación otorgada de 60 puntos y la ausencia de evidencias documentales en el repositorio que demuestren la aplicación o seguimiento de estos procedimientos, se recomienda adelantar acciones que fortalezcan la implementación y trazabilidad del proceso disciplinario en casos de incumplimiento a las políticas de seguridad de la información.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
				investigaciones. En coherencia con este lineamiento, se considera que la entidad dispone de una base normativa que regula las sanciones frente a vulneraciones en materia de seguridad de la información.	
P.1.5	A 6.5	Responsabilidades después de la finalización o cambio de empleo	40	De acuerdo con la revisión efectuada, la Guía de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC contempla lineamientos asociados a la gestión de responsabilidades de seguridad de la información posteriores a la terminación o cambio de empleo, en concordancia con lo establecido en este control.	En referencia a la calificación otorgada de 40 puntos, se recomienda al responsable del MSPI realizar revisión de la documentación asociada, así como adelantar las acciones necesarias que garanticen su aplicación y cumplimiento efectivo dentro del proceso de gestión de talento humano y contratación.
P.1.6	A 6.6	Acuerdos de confidencialidad o no divulgación	40	Se observa que la Guía de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC contempla en el numeral 4.9.3.3 "Acuerdos de Confidencialidad o No Divulgación" la obligación de establecer, revisar y documentar los requisitos aplicables a los acuerdos de confidencialidad que garanticen la protección de la información institucional. Asimismo, se dispone que en todos los convenios o contratos suscritos por la entidad con funcionarios, contratistas y demás personal, se debe incluir una cláusula de confidencialidad y reserva de la información.	Al no identificarse soportes documentales en el repositorio que acrediten el cumplimiento integral de este criterio, y considerando la calificación otorgada de 40 puntos, se recomienda adelantar las acciones necesarias para evidenciar la aplicación y trazabilidad de los acuerdos de confidencialidad en todos los contratos y vínculos vigentes, asegurando su actualización conforme a los lineamientos de la guía.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
P.1.7	A 6.7	Trabajo remoto	40	En seguimiento a este criterio, se evidencia que la Guía de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC, en su numeral 4.2.2.2 "Teletrabajo", establece los lineamientos para garantizar la seguridad de la información y la eficiencia operativa en los entornos de trabajo remoto. La guía dispone que la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) debe realizar inspecciones técnicas a los puestos de trabajo, asegurar el uso de servicios de antivirus, respaldo, acceso seguro mediante VPN y definir políticas que garanticen los principios de confidencialidad, integridad, disponibilidad y autenticación.	Considerando la calificación otorgada de 40 puntos, se sugiere fortalecer las acciones asociadas a la implementación y seguimiento de las medidas técnicas y administrativas para el teletrabajo de acuerdo con lo descrito en la guía, con el fin de garantizar la protección de la información y la continuidad operativa bajo esta modalidad.
P.1.8	A 6.8	Reporte de eventos de seguridad de la información	40	El proceso de Gestión TIC cuenta con la Guía de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios TIC, así como con el Manual de Gestión de Incidentes de Seguridad de la Información, los cuales establecen los lineamientos a seguir cuando se presentan incidentes o eventos. Adicionalmente, y de acuerdo con validación realizada con el Oficial de Seguridad de la Información, se dispone de una bitácora de eventos en la que, para las vigencias 2024 y 2025, se han registrado 17 ítems. Lo anterior evidencia gestión respecto a este criterio.	De acuerdo con la calificación otorgada de 40 puntos, bajo el argumento de que se requiere actualizar el procedimiento, se sugiere al proceso continuar y adelantar las acciones necesarias en pro del fortalecimiento y el cumplimiento de este criterio.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Dominio controles físicos:

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
F.1.1	A 7.1	Perímetros de seguridad física	40	En seguimiento a este criterio, se evidencia que la entidad dispone de lineamientos establecidos en la Guía de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC, donde se contemplan disposiciones relacionadas con el control de acceso físico, la protección de las instalaciones y la custodia de los activos tecnológicos.	Sin embargo, considerando la calificación otorgada de 40 puntos, se propone fortalecer la evidencia documental que soporte la aplicación de dichas medidas, especialmente las referidas a controles de ingreso, bitácoras de acceso y mecanismos de protección física en las áreas críticas.
F.1.2	A 7.2	Entrada física	60	Se evidencia que la entidad cuenta con mecanismos de control de acceso físico que incluyen la utilización de tarjetas de proximidad y carné institucional de identificación para todo el personal, garantizando una movilidad controlada dentro de las instalaciones. El acceso al centro de cómputo se encuentra debidamente restringido al personal autorizado de la Oficina TIC (OTIC), responsable de su operación y mantenimiento. Adicionalmente, se implementan controles complementarios como el registro de ingreso y salida de equipos de cómputo en el edificio principal de la Alcaldía, medida que contribuye a prevenir la pérdida o salida no autorizada de activos tecnológicos. En este contexto, los controles de acceso físico se encuentran implementados y operando de manera efectiva, sin evidenciarse incidentes o pérdidas asociadas.	Considerando la calificación actual de 60 puntos, se recomienda culminar las acciones pendientes orientadas al fortalecimiento del control y realizar una nueva evaluación de la calificación, en coherencia con el nivel de efectividad demostrado.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
F.1.3	A 7.3	Aseguramiento de oficinas, salas e instalaciones	60	La guía de seguridad contempla la protección física y del entorno en el numeral 4.7 La OTIC otorga calificación de 60. Adicional indica que las oficinas de la entidad están aseguradas por puertas que se pueden abrir con tarjetas de proximidad asignadas a todo el personal, complementariamente se informa que el centro de cómputo se controla con acceso biométrico.	Por lo informado se propone revisar la valoración actual y continuar con el desarrollo de las actividades orientadas a fortalecer el control de aseguramiento de oficinas, salas e instalaciones. Dichas acciones deben adelantarse conforme a los lineamientos definidos en la Guía de Seguridad y Privacidad de la Información (numeral 4.7.1.2 – Control de Acceso Físico de Entrada), garantizando la continuidad, efectividad y mejora de las medidas implementadas en materia de seguridad física y control de acceso.
F.1.4	A 7.4	Supervisión de la seguridad física	60	Se evidencia que la entidad dispone de mecanismos de supervisión y monitoreo físico, tales como sistemas de videovigilancia, alarmas contra intrusión y controles de acceso restringido, los cuales permiten vigilar de manera continua las áreas críticas y detectar posibles eventos no autorizados. Los sistemas instalados cumplen con las disposiciones establecidas en la Guía de Seguridad y Privacidad de la Información (código 2310200-GS-013, numeral 4.7.1.3 “Supervisión de la Seguridad Física”), que orienta la implementación de medidas preventivas y reactivas para salvaguardar las instalaciones y los activos tecnológicos.	De acuerdo con la calificación otorgada de 60 puntos, se considera que el control se encuentra implementado y operando; no obstante, se recomienda fortalecer la evidencia documental y la justificación que respalde el cumplimiento de este criterio.
F.1.5	A 7.5	Protección contra amenazas físicas y ambientales	60	Se evidencia que la entidad dispone de sistemas operativos de detección de incendios y de extintores con fechas de recarga vigentes, lo cual refleja la aplicación de controles preventivos frente a amenazas	En este contexto, y considerando la calificación otorgada de 60 puntos, se determina que el control presenta un nivel de cumplimiento aceptable. No obstante, se recomienda

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
				físicas y ambientales. La Guía de Seguridad y Privacidad de la Información (código 2310200-GS-013), en su numeral 4.7.1.3 "Protección contra amenazas ambientales", establece las acciones requeridas para mitigar los riesgos asociados con incendios, inundaciones, sismos y otros eventos, incluyendo la identificación y almacenamiento controlado de materiales combustibles, el aseguramiento del mobiliario y de los elementos susceptibles de causar daño físico, así como la formulación y puesta en marcha de planes de respuesta y de protección del personal ante emergencias.	fortalecer y documentar las actividades complementarias que consoliden la gestión preventiva, asegurando el cumplimiento integral de los lineamientos institucionales y promoviendo la mejora continua en la protección contra amenazas físicas y ambientales
F.1.6	A 7.6	Trabajar en áreas seguras	60	Las oficinas de la Secretaría Jurídica Distrital cuentan con controles de acceso físico implementados, mediante el uso de tarjetas de proximidad y lector biométrico para el ingreso al centro de cómputo, administrado por la Oficina de Tecnologías de la Información (OTIC). Los lineamientos institucionales definidos en la Guía de Seguridad y Privacidad de la Información (código 2310200-GS-013), particularmente en los numerales 4.7.1 "Áreas Seguras" y 4.7.1.4 "Seguridad en Oficinas y Áreas de Trabajo", establecen directrices específicas orientadas a la prevención de accesos no autorizados, la supervisión de actividades en zonas restringidas, la limitación en el uso de equipos de grabación y la exigencia de portar identificación visible tanto para el personal interno como para los visitantes.	En concordancia con el seguimiento realizado y considerando la calificación actual de 60 puntos, se considera pertinente fortalecer la documentación soporte y evidencias que respalden la aplicación continua de los controles establecidos, así como avanzar en la implementación de actividades complementarias que consoliden la gestión de seguridad física. Estas acciones permitirán asegurar el cumplimiento integral de los lineamientos institucionales y promover la madurez del control asociado al trabajo en áreas seguras.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
F.1.7	A 7.7	Escritorio despejado y pantalla despejada	60	Se evidencia que la Secretaría Jurídica Distrital cuenta con una Política de Escritorio y Pantalla Limpia, establecida en el numeral 4.7.2.6 de la Guía de Seguridad y Privacidad de la Información (código 2310200-GS-013), la cual define las directrices que deben cumplir todos los funcionarios para garantizar la protección de la información institucional. Esta política dispone que el personal debe mantener su espacio de trabajo libre de documentos o medios que contengan información sensible, bloquear la pantalla del equipo al ausentarse, apagar la estación de trabajo al finalizar la jornada, y asegurar bajo llave la información clasificada o reservada. Asimismo, establece la obligación de retirar de inmediato los documentos de equipos de reproducción como impresoras o escáneres, evitando la exposición no autorizada de información.	En este contexto, y considerando la calificación actual de 60 puntos, resulta recomendable fortalecer los mecanismos de socialización, seguimiento y registro documental que evidencien la aplicación efectiva de esta política.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
F.1.8	A 7.8	Ubicación y Protección del equipo	60	La Secretaría Jurídica Distrital cuenta con lineamientos establecidos en la Guía de Seguridad y Privacidad de la Información (código 2310200-GS-013), particularmente en los numerales 4.7.2 "Ubicación y Protección de Equipos" y subsiguientes, que definen medidas para la protección física y eléctrica de la infraestructura tecnológica, la seguridad del cableado, el mantenimiento preventivo y correctivo, y los procedimientos para el retiro controlado de activos. La Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) ejecuta mantenimientos conforme a un cronograma establecido, dispone de estaciones de trabajo con conexiones eléctricas reguladas y cableado protegido mediante canaletas, contribuyendo a la conservación de los activos tecnológicos.	En este sentido, se valida la existencia de controles físicos y eléctricos operativos, como sistemas de protección ante fallas eléctricas y mecanismos de registro para el retiro de equipos. No obstante, considerando la calificación de 60 puntos, se recomienda fortalecer la evidencia documental y verificar la aplicación integral de los lineamientos, especialmente en lo relativo al monitoreo de condiciones ambientales, protección del cableado y mantenimiento programado, con el fin de elevar el nivel de cumplimiento y garantizar la continuidad operativa en condiciones seguras.
F.1.9	A 7.9	Seguridad de los activos fuera de las instalaciones	40	La entidad cuenta con lineamientos definidos para la seguridad de los equipos fuera de las instalaciones, según la Guía de Seguridad y Privacidad de la Información. Estos establecen medidas como el cifrado de datos, aseguramiento físico, desactivación de conexiones inalámbricas y reporte inmediato de pérdidas o robos.	En relación a la calificación asignada de 40 puntos, se aconseja fortalecer la aplicación y evidencia de estas políticas, especialmente en el registro y seguimiento de equipos, capacitación del personal y adopción de medidas complementarias, con el fin de reducir riesgos y mejorar el nivel de cumplimiento del control.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
F.1.10	A 7.10	Medios de almacenamiento	40	Se evidencia que la Secretaría Jurídica Distrital cuenta con lineamientos para la gestión de medios de almacenamiento definidos en el numeral 4.4.3 de la Guía de Seguridad y Privacidad de la Información, los cuales establecen controles para proteger la información en unidades removibles y medios físicos, garantizando su confidencialidad, integridad y disponibilidad. La OTIC es responsable de regular su uso, restringir dispositivos no autorizados y aplicar medidas como el cifrado y registro de retiro de medios.	En consideración con la calificación de 40 puntos, se resalta fortalecer la implementación y evidencia de las actividades, formalizando la autorización y trazabilidad del manejo de medios, aplicando controles criptográficos (en casi de aplicar) y verificando las condiciones de almacenamiento y eliminación segura, con el fin de reducir riesgos de fuga o pérdida de información y mejorar el nivel de cumplimiento del control.
F.1.11	A 7.11	Servicios de apoyo	40	No se identifican dentro de la documentación institucional lineamientos o políticas asociadas al cumplimiento de este control. Asimismo, en el instrumento MSPI el responsable del modelo no reporta información ni evidencia que respalde la gestión del requisito, manteniendo una calificación de 40. Esta situación refleja que el aspecto continúa con bajo nivel de avance y sin evidencias verificables.	Una vez ejecutado el seguimiento a este criterio se considera pertinente fortalecer la documentación y registro de soportes que demuestren el cumplimiento del control, garantizando su trazabilidad dentro del modelo.
F.1.12	A 7.12	Seguridad del cableado	60	El tema de cableado, se contempla en la guía de seguridad en el numeral 4.7.2.4 el cual menciona lineamientos de protección, separación de rutas y marcación.	Aunque la calificación otorgada por la OTIC es de 60, se considera necesario fortalecer las actividades de seguimiento y documentación técnica que respalden la aplicación integral de los lineamientos. El fortalecimiento de estos aspectos contribuirá a incrementar el nivel de cumplimiento, consolidar la confiabilidad del cableado estructurado y garantizar la continuidad y protección de los

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
					servicios tecnológicos de la entidad.
F.1.13	A 7.13	Mantenimiento de equipos	60	Se identifica que la OTIC) ha formalizado el Procedimiento 2310200-PR-095 "Mantenimiento de Equipos de Cómputo", ejecutado conforme al Cronograma 2310200-FT-276, lo que garantiza la planeación y realización periódica de mantenimientos preventivos y correctivos. Este proceso se encuentra alineado con la Guía de Seguridad y Privacidad de la Información (código 2310200-GS-013, numeral 4.7.2.5 "Mantenimiento a los Equipos"), que establece la obligación de realizar mantenimientos regulares, conservar los registros de intervención y asegurar que las actividades sean desarrolladas por personal autorizado.	Si bien la calificación actual de 60 puntos refleja avances en la formalización del proceso, se sugiere fortalecer la trazabilidad y la evidencia documental de las actividades realizadas y describir la justificación dentro del instrumento acorde a la realidad operativa.
F.1.14	A 7.14	Eliminación segura o reutilización de equipos	40	En el control "Eliminación segura o reutilización de equipos", se evidencia que la Secretaría Jurídica Distrital cuenta con lineamientos establecidos en la Guía de Seguridad y Privacidad de la Información (código 2310200-GS-013), orientados a asegurar la disposición adecuada de equipos y medios de almacenamiento que contengan información institucional. Estos lineamientos incluyen el uso de técnicas de borrado seguro de datos, la verificación previa del contenido antes de su eliminación o reutilización, y la supresión de etiquetas o marcas institucionales antes de su disposición final, reubicación o donación.	De acuerdo con lo informado y dado que la calificación asignada para la presente vigencia es de 40, se indica fortalecer las evidencias y los soportes, así como también la justificación de cumplimiento que se describe dentro del instrumento MSPI.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Dominio controles tecnológicos:

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
T.1.1	A 8.1	Dispositivos de punto final de usuario	40	En el seguimiento al control sobre la configuración y manejo seguro de los dispositivos de punto final, se identificó que la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) otorgó una calificación de 40 puntos, sin aportar evidencias que respalden el cumplimiento del criterio. La Guía 2310200-GS-013 establece lineamientos aplicables en los numerales 4.2.2.1 "Política para Dispositivos Móviles" y 4.2.2.2 "Teletrabajo", orientados a la gestión segura de los dispositivos, se evidencian brechas en la documentación, formalización y seguimiento de las acciones ejecutadas.	Derivado de la calificación asignada por la OTIC la cual es de 40, se propone fortalecer las evidencias y los soportes, así como también la justificación de cumplimiento que se describe dentro del instrumento MSPI.
T.1.2	A 8.2	Derechos de acceso privilegiado	40	En el seguimiento efectuado al control sobre los derechos de acceso privilegiado, se evidenció que la Secretaría Jurídica Distrital cuenta con el procedimiento "Administración de Usuarios y Gestión de Accesos", el cual define lineamientos para la asignación, control y revisión de privilegios en los sistemas de información. De igual forma, la Guía 2310200-GS-013 establece directrices orientadas a garantizar la autorización, trazabilidad y temporalidad de dichos accesos.	En concordancia con lo mencionado en el seguimiento, la OTIC otorgó una calificación de 40 puntos, sin evidencias suficientes que respalden el nivel de cumplimiento reportado. En este sentido, se recomienda revisar la calificación y realizar un nuevo análisis sustentado en documentación verificable y en la efectividad real de los controles aplicados.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
T.1.3	A 8.3	Restricción de acceso a la información	40	En el seguimiento realizado al control de restricción de acceso a la información, se evidenció que las aplicaciones utilizadas por la Secretaría Jurídica Distrital gestionan los permisos a través de roles y perfiles de usuario.	Se considera pertinente revisar y reevaluar la calificación, sustentándola en evidencias técnicas, registros de control y trazabilidad de accesos que permitan determinar con mayor precisión el grado real de cumplimiento. Así mismo, se sugiere fortalecer la gestión del control de accesos, mediante la verificación periódica de privilegios, y asegurar que la asignación, modificación y revocación de permisos se realicen de acuerdo con los lineamientos institucionales y las buenas prácticas de seguridad de la información establecidas en la Guía 2310200-GS-013, garantizando una protección efectiva de la información durante todo su ciclo de vida.
T.1.4	A 8.4	Acceso al código fuente	20	En el seguimiento realizado al control de restricción de acceso a la información, se evidenció que las aplicaciones utilizadas por la Secretaría Jurídica Distrital gestionan los permisos a través de roles y perfiles, no obstante, la OTIC otorgó una calificación de 40 puntos, sin que se cuente con evidencias documentales suficientes que respalden el nivel de cumplimiento reportado.	De acuerdo con lo reportado en el seguimiento es recomendable revisar y reevaluar la calificación, sustentándola en evidencias técnicas, registros de control y trazabilidad de accesos que permitan determinar con mayor precisión el grado real de cumplimiento. Así mismo, se sugiere fortalecer la gestión del control de accesos, mediante la verificación periódica de privilegios, y asegurar que la asignación, modificación y revocación de permisos se realicen de acuerdo con los lineamientos institucionales y las buenas prácticas de seguridad de la información establecidas en la Guía 2310200-GS-013, garantizando una protección efectiva de la información durante todo su ciclo de vida.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
T.1.5	A 8.5	Autenticación segura	40	En la revisión del control "Autenticación segura", se evidenció que la Guía de Seguridad y Privacidad de la Información (2310200-GS-013) define principios y responsabilidades sobre el uso de identificadores únicos, gestión de privilegios, trazabilidad y control de accesos remotos. Asimismo, en la auditoría al proceso de Gestión de Talento Humano se constató un avance en la gestión de contraseñas en PERNO, incorporando parámetros de complejidad, caducidad y cambio periódico, lo que refleja mejoras en la protección de los accesos institucionales.	No obstante y considerando la calificación de 40 puntos otorgada por la OTIC, se plantea la necesidad de revisar y actualizar la evaluación realizada, así como también ejecutar un diagnóstico integral de los mecanismos de autenticación en todos los sistemas de información, a fin de identificar brechas y fortalecer el cumplimiento de los requisitos establecidos para la autenticación segura.
T.1.6	A 8.6	Gestión de la capacidad	40	En la revisión del control "Gestión de la capacidad", se constató que la Guía de Seguridad y Privacidad de la Información (2310200-GS-013), en su numeral 4.8.1.2, define directrices para garantizar la disponibilidad, eficiencia y continuidad de los servicios TIC, promoviendo el monitoreo, la planeación y la adopción de medidas preventivas ante posibles limitaciones.	Derivado del seguimiento y considerando la calificación de 40 puntos otorgada por la OTIC, se propone revisar y reevaluar el puntaje y de manera complementaria fortalecer la gestión de capacidad mediante la implementación de mecanismos de medición, monitoreo y registro continuo de los recursos tecnológicos, garantizando el cumplimiento de los lineamientos definidos en la guía institucional y la mejora del desempeño operativo.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
T.1.7	A 8.7	Protección contra malware	40	En el seguimiento al control "Protección contra malware", se verificó que la Guía de Seguridad y Privacidad de la Información (2310200-GS-013), en su numeral 4.8.2, establece la obligación de aplicar medidas preventivas, detectivas y correctivas frente al código malicioso. La OTIC reporta el uso de Windows Defender en las estaciones de trabajo como sistema de antivirus.	Considerando la calificación de 40 puntos, es recomendable revisar el puntaje asignado y gestionar la documentación y justificación derivado de este aspecto en el instrumento MSPI.
T.1.8	A 8,8	Gestión de vulnerabilidades técnicas	40	En el seguimiento al control "Gestión de vulnerabilidades técnicas", se evidenció que la entidad ha avanzado en la identificación y análisis de vulnerabilidades en los principales sistemas institucionales (Alfresco, Bizagi, Drupal, Liquidador de Nómina, entre otros), mostrando mejoras durante la vigencia 2025.	De acuerdo con el numeral 4.8.3.1 de la Guía 2310200-GS-013, se recomienda fortalecer la documentación y evidencias en el MSPI, incorporando los resultados y mecanismos de gestión de vulnerabilidades aplicados por la OTIC. Considerando la calificación de 40 puntos, se sugiere revisar y ajustar el puntaje en función de los avances técnicos alcanzados y la efectividad de las acciones implementadas.
T.1.9	A 8.9	Gestión de la configuración	40	La revisión del control "Gestión de la configuración" evidencia que la Oficina TIC asignó una calificación de 40 puntos sin aportar documentación de soporte, descripciones de cumplimiento ni evidencias que respalden dicha valoración. Asimismo, en el repositorio institucional no se encontraron registros o evidencias asociadas al control. La Guía de Seguridad y Privacidad de la Información (2310200-GS-013) no establece lineamientos técnicos sobre gestión de configuraciones ni el uso de plantillas o parámetros estandarizados, lo que	Se sugiere revisar integralmente la calificación otorgada en el instrumento MSPI, así como la documentación de las prácticas efectivas de configuración, los procedimientos directamente relacionados con el control, acordes a la realidad operativa en la plataforma tecnológica de la entidad.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
				representa una brecha frente al criterio de evaluación.	
T.1.10	A 8.10	Eliminación de información	0	Según lo reportado por la OTIC en el instrumento MSPI, la entidad no ha generado evidencia ni documentación sobre la implementación del control de Eliminación de Información. No se identifican procedimientos, registros de borrado ni seguimiento a proveedores externos. La Guía de Implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los Servicios TIC tampoco aborda este tema.	Para este criterio la OTIC asigna una calificación de 0 punto, ante esto es aconsejable desarrollar e implementar actividades específicas para cumplir con este control.
T.1.11	A 8.11	Enmascaramiento de datos	0	Según lo reportado por la OTIC en el instrumento MSPI, la entidad no ha diligenciado información ni generada evidencia sobre la implementación del control de enmascaramiento de datos, reportando una calificación de 0. Además, la Guía de Implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los Servicios TIC no incluye un apartado relacionado con este control.	Ante lo descrito, se propone que la entidad desarrolle e implemente actividades para cumplir con este criterio, así como la generación, registro y conservación de evidencias que respalden la protección de los datos y faciliten el seguimiento del control.
T.1.12	A 8.12	Prevención de fuga de datos	20	En la revisión del instrumento MSPI, la entidad reporta una calificación de 20 para el control de Prevención de Fuga de Datos, sin presentar evidencia ni justificación que respalde dicha puntuación, ni se identifican avances o acciones concretas para cumplir plenamente con el control.	Se recomienda que la entidad implemente actividades para cumplir este control, incluyendo la identificación y clasificación de información sensible, el monitoreo de posibles fugas y la generación de evidencias que demuestren la efectividad de las medidas adoptadas, con el fin de mitigar riesgos de divulgación no autorizada y fortalecer la seguridad de la información.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
T.1.13	A 8.13	Copia de seguridad de la información	20	En la auditoría realizada sobre el sistema SICAPITAL, específicamente a PERNO en las vigencias 2024 y 2025, se verificó la existencia y ejecución de copias de seguridad, respaldadas por el documento 2310200-PR-046 "Administración de Backups y Restore". La Guía de Seguridad (apartado 4.8.3) establece requisitos sobre frecuencia, almacenamiento seguro, pruebas periódicas y registro de ejecución, los cuales aún no se aplican plenamente. Por lo anterior, la OTIC reporta una calificación de 20.	Derivado del seguimiento realizado es recomendable que la OTIC realice un diagnóstico general de todos los sistemas de información para determinar un grado más preciso de cumplimiento del control asociado a copias de seguridad, incluyendo la generación y registro de documentación, evidencias de ejecución y pruebas de restauración periódicas, con el fin de fortalecer la seguridad de la información y garantizar la disponibilidad de los sistemas críticos ante incidentes.
T.1.14	A 8.14	Redundancia de las instalaciones de procesamiento de información	20	En la revisión del instrumento MSPI, la entidad reporta una calificación de 20 para el control de redundancia de las instalaciones de procesamiento de información, sin aportar evidencia ni información que respalde dicha puntuación, ni indicar avances o aspectos pendientes para cumplir plenamente el control. Si bien se tienen copias de seguridad y se están subiendo servicios a nube, la entidad continua con servidores físicos.	Se propone que la OTIC realice un diagnóstico de todas las instalaciones de procesamiento de información, verificando la existencia y operación de componentes redundantes, procedimientos de conmutación por error, seguridad de los sistemas duplicados y documentación de evidencias que respalden estas prácticas. Estas acciones fortalecerán la disponibilidad de los servicios y garantizarán la continuidad operativa de los sistemas críticos.
T.1.15	A 8.15	Registro	20	En la revisión del instrumento MSPI, la entidad reporta una calificación de 20 para el control de registro, sin aportar evidencia ni información que respalde la puntuación, ni indicar avances o aspectos pendientes para cumplir plenamente el control. La Guía de Seguridad (apartado 4.8.4) establece que todos los eventos en los sistemas de información deben contar con registros de auditoría que	Se propone que la OTIC realice un diagnóstico de todos los sistemas para evaluar la implementación de los registros de eventos, incluyendo generación de evidencias, verificación de integridad y protección de los registros, y aplicación de procedimientos de análisis y monitoreo según la guía. Estas acciones fortalecerán la trazabilidad, el

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
				incluyan excepciones y otros eventos relacionados con la seguridad, lo cual aún requiere validación y documentación completa.	análisis de incidentes y la seguridad de la información
T.1.16	A 8.16	Actividades de seguimiento	40	La entidad reporta una calificación de 40 para Actividades de Seguimiento y 20 para Registro, ambos alineados con la Guía de Seguridad (apartado 4.8.4). No obstante, no se presentan evidencias que respalden la ejecución efectiva de las actividades ni la implementación de los registros y monitoreo asociados.	Ante lo descrito e identificado en el seguimiento se sugiere que la OTIC realice un diagnóstico de todos los sistemas de información, generando evidencias y documentación que respalden la efectividad de los controles, asegurando la correlación de eventos y fortaleciendo la gestión integral de seguridad de la información.
T.1.17	A 8.17	Sincronización del reloj (clock)	60	La OTIC reporta una calificación de 60 para el control de sincronización del reloj. No obstante, auditorías a sistemas como el módulo PERNO de SICAPITAL durante 2024 y 2025 evidenciaron desalineación con la hora legal colombiana, lo que podría afectar la precisión de los registros de eventos y su validez como evidencia.	Para este caso es importante que la OTIC implemente procedimientos para sincronizar todos los sistemas con una fuente de tiempo confiable vinculada a la hora legal, y que genere y conserve evidencias que respalden la ejecución y verificación de esta sincronización, garantizando el cumplimiento del control y la confiabilidad de los registros de auditoría.
T.1.18	A 8.18	Uso de programas de utilidad privilegiados	40	La OTIC reporta una calificación de 40, indicando que es la única dependencia que realiza la configuración e instalación de programas en los computadores de los colaboradores, siguiendo la línea base de software definida por la entidad. Sin embargo, la Guía de Seguridad (apartado 4.8.5.1) establece que los funcionarios no deben instalar software en sus equipos, reforzando la necesidad de un control estricto sobre el uso de programas de utilidad.	Ante lo descrito es recomendable que la OTIC implemente actividades que garanticen el cumplimiento de este criterio, incluyendo documentación y generación de evidencias que respalden la autorización, instalación y uso de software privilegiado, asegurando trazabilidad y efectividad de los controles.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
T.1.19	A 8.19	Instalación de software en sistemas operativos	40	La OTIC reporta una calificación de 40, indicando que es la única dependencia que realiza la configuración e instalación de programas en los computadores de los colaboradores, siguiendo la línea base de software de la entidad. Sin embargo, la Guía de Seguridad (numeral 4.8.5.1) establece que los funcionarios no deben instalar software en sus equipos, reforzando la necesidad de controlar estrictamente el uso de programas de utilidad.	Con base en la validación de este criterio, es conveniente que la OTIC implemente las actividades necesarias para garantizar el cumplimiento del control, incluyendo documentación y generación de evidencias que respalden la autorización, instalación y uso de software privilegiado, asegurando trazabilidad y efectividad de los controles.
T.1.20	A 8.20	Seguridad en redes	60	La OTIC reporta una calificación de 60, indicando que la administración de las redes de la entidad está a cargo de dicha oficina, con segmentación mediante VLANs, control de acceso a servicios expuestos a internet mediante firewall, y asignación de credenciales personales y trazables. La Guía de Seguridad y Privacidad de la Información (numerales 4.5.1.2, 4.9.1 y 4.9.2) establece lineamientos sobre acceso a redes, gestión de seguridad, segregación y asignación de privilegios, incluyendo autenticación segura y control de puertos y dispositivos.	Por la importancia de este aspecto, la OTIC debe priorizar la ejecución de las actividades necesarias para garantizar el cumplimiento, generando documentación y evidencias que respalden la seguridad de redes y el cumplimiento de los requisitos de acceso, segregación y monitoreo de la infraestructura.
T.1.21	A 8.21	Seguridad de los servicios de red	60	La OTIC reporta una calificación de 60, indicando que la administración de las redes está a cargo de la Oficina TIC, con segmentación mediante VLANs, control de acceso a servicios expuestos a internet por firewall, y asignación de credenciales personales y trazables. La Guía de Seguridad y Privacidad de la Información (numerales 4.5.1.2, 4.9.1 y 4.9.2) establece lineamientos sobre acceso a	Se considera pertinente que la OTIC implemente las actividades necesarias para garantizar el cumplimiento efectivo del control, generando documentación y evidencias que respalden la seguridad de redes y el cumplimiento de los requisitos de acceso, segregación y monitoreo de la infraestructura.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
				redes, gestión de seguridad, segregación y asignación de privilegios, incluyendo autenticación segura y control de puertos y dispositivos.	
T.1.22	A 8.22	Segregación de redes	60	La OTIC reporta una calificación de 60, indicando que la administración de las redes está a cargo de la Oficina TIC, con segmentación mediante VLANs, control de acceso a servicios expuestos a internet mediante firewall y asignación de credenciales personales y trazables. La Guía de Seguridad y Privacidad de la Información (numerales 4.5.1.2, 4.9.1 y 4.9.2) establece lineamientos sobre acceso a redes, gestión de seguridad, segregación y asignación de privilegios, incluyendo autenticación segura y control de puertos y dispositivos.	Ante esto, la OTIC debe ejecutar las actividades necesarias para asegurar el cumplimiento del control, generando documentación y evidencias que respalden la seguridad de redes y el cumplimiento de los requisitos de acceso, segregación y monitoreo de la infraestructura
T.1.23	A 8.23	Filtrado web	40	La OTIC reporta una calificación de 40 para este control; sin embargo, el instrumento no detalla cómo se implementa el filtrado web ni identifica brechas o aspectos pendientes para su cumplimiento. Adicional en validación, se identifica que al navegar en internet no hay restricciones para acceso a páginas de juegos, apuestas en línea, transferencia de información entre otros.	Por la importancia del tema, la se recomienda que la OTIC priorice este tema para que de manera efectiva y siguiendo los lineamientos de la guía de seguridad y las mejores prácticas, se ejecuten las actividades asociadas, así como también se generen los soportes y evidencias que respalden su ejecución. Posteriormente, se sugiere reevaluar la calificación para reflejar el nivel real de cumplimiento.
T.1.24	A 8.24	Uso de criptografía	0	La OTIC reporta una calificación de 0 para este control, sin evidencias que respalden la implementación de políticas, gestión de claves o uso adecuado de criptografía.	Se recomienda que la entidad identifique los sistemas, aplicaciones y datos que requieren protección mediante criptografía, y que, con base en este diagnóstico, desarrolle e implemente políticas, estándares de criptografía, gestión segura de claves y

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
					registro de actividades. Es fundamental generar evidencias que demuestren el cumplimiento efectivo del control y reevaluar posteriormente la calificación de manera objetiva.
T.1.25	A 8.25	Ciclo de vida de desarrollo seguro	20	La OTIC reporta una calificación de 20, indicando que algunos sistemas de información no cuentan con los tres ambientes requeridos (desarrollo, pruebas y producción). .	Ante esto se sugiere identificar los sistemas que disponen de los tres ambientes y aquellos que carecen de alguno, a fin de planear acciones para cumplir con los criterios de desarrollo seguro establecidos en la guía de seguridad (numeral 4.10.2). Esta actividad debe documentarse, generando soportes y evidencias que permitan verificar su cumplimiento y fortalecer la seguridad en el ciclo de vida del desarrollo de software
T.1.26	A 8.26	Requisitos de seguridad de la aplicación	20	La OTIC reporta una calificación de 20, indicando que aunque los lineamientos están definidos en la Guía de Seguridad 2310200-GS-013 (numeral 4.10), no se evidencian soportes que demuestren la aplicación efectiva de los requisitos de seguridad en las aplicaciones de la entidad.	Con base en el seguimiento, se propone identificar y documentar los requisitos de seguridad específicos para cada aplicación, incluyendo autenticación, confidencialidad, integridad, segregación de acceso, protección de transacciones y cumplimiento legal. Además, se debe generar y conservar evidencia que respalde el cumplimiento de estos requisitos y, con base en ella, estimar de manera objetiva la calificación de cada sistema, fortaleciendo la seguridad de las aplicaciones y el cumplimiento de la guía.
T.1.27	A 8.27	Arquitectura del sistema seguro y principios de ingeniería	20	La OTIC reporta una calificación de 20 para este control; sin embargo, no se evidencian soportes que sustenten la calificación ni se hace referencia explícita a los lineamientos de la Guía de Seguridad 2310200-	Derivado de lo descrito, resulta conveniente elaborar un texto de justificación detallado que explique los motivos de la calificación asignada, incluyendo los controles aplicados, las prácticas de ingeniería segura

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
				GS-013 relacionados con principios de ingeniería segura.	implementadas y las limitaciones identificadas. Esta documentación permitirá respaldar la calificación, garantizar la trazabilidad de las decisiones de seguridad y orientar las acciones necesarias para cumplir con los principios de arquitectura de sistemas seguros establecidos en la guía.
T.1.28	A 8.28	Codificación segura	0	La OTIC no reporta avances ni evidencia sobre la implementación de prácticas de codificación segura.	Para este aspecto cabe enfatizar en desarrollar actividades de documentación así como de sustentar las actividades realizadas en todas las etapas del ciclo de desarrollo planificación, codificación, pruebas y mantenimiento generando evidencias que respalden la calificación del control y fortalezcan la gobernanza de la codificación segura.
T.1.29	A 8.29	Pruebas de seguridad en desarrollo y aceptación	0	La OTIC reporta una calificación de 0, evidenciando ausencia de gestión en la aplicación de pruebas de seguridad durante el desarrollo o aceptación de los sistemas de información. La Guía de Seguridad y Privacidad de la Información (2310200-GS-013, capítulo 4.10.2.6) establece lineamientos para pruebas de seguridad, incluyendo estandarización del ciclo de vida del software, criterios de calidad y seguridad, uso de datos de prueba, y pruebas de compatibilidad, integración, funcionalidad, desempeño e instalación. La entidad cuenta con directrices definidas, pero se requiere su aplicación práctica y seguimiento documentado.	Para este criterio, cabe informar que se recomienda debe generar evidencia que respalde el cumplimiento de este control, así como la justificación que se describe en el instrumento MSPI.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
T.1.30	A 8.30	Desarrollo subcontratado	0	La OTIC reporta una calificación de 0, evidenciando ausencia de acciones para gestionar la seguridad en desarrollos de sistemas subcontratados.	Se aconseja establecer lineamientos y requisitos contractuales que incluyan prácticas seguras de diseño, codificación y pruebas, así como mecanismos de monitoreo y aseguramiento que garanticen la calidad y seguridad de los entregables de los proveedores. Asimismo, se sugiere documentar evidencias y resultados que respalden la implementación progresiva de este control.
T.1.31	A 8.31	Separación de los entornos de desarrollo, prueba y producción	0	La OTIC reporta una calificación de 0, indicando que algunos sistemas de información no cuentan con los tres ambientes requeridos (desarrollo, pruebas y producción).	Frente a este tema, se considera pertinente identificar los sistemas que disponen de los tres ambientes y aquellos que carecen de alguno, a fin de planear acciones para cumplir con los criterios de desarrollo seguro establecidos en la guía de seguridad (numeral 4.10.2). Esta actividad debe documentarse, generando soportes y evidencias que permitan verificar su cumplimiento y fortalecer la seguridad en el ciclo de vida del desarrollo de software.
T.1.32	A 8.32	Gestión de cambios	40	Aunque la OTIC reporta calificación de 40, la Guía de Seguridad establece el procedimiento 2310200-PR-096 Gestión de Control de Cambios de Servicios de TI.	Teniendo en cuenta la gestión adelantada por la OTIC, en referencia este tema y la calificación de 40, se recomienda revisar la calificación, y para tal fin, adjuntando las evidencias y justificando el motivo por el cual se cumple en ese nivel y adicionando la brecha o temas pendientes,

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación OTIC)	Comentario OCI	Análisis valoración OTIC Recomendaciones
T.1.33	A 8.33	Información de prueba	20	La entidad reporta una calificación de 20, indicando que la Guía de Seguridad y Privacidad de la Información (2310200-GS-013, numeral 4.10.2.6) establece lineamientos para la protección de la información en pruebas. Sin embargo, no se evidencia cómo se aplica este control en los sistemas ni la gestión práctica implementada.	Debido a la calificación de 20 puntos, se recomienda documentar y evidenciar la aplicación de estos lineamientos en los entornos de prueba, así como también se sugiere revisar la calificación otorgada para reflejar la implementación efectiva del control.
T.1.34	A 8.34	Protección de los sistemas de información durante las pruebas de auditoría	20	La OTIC reporta una calificación de 20, sin presentar justificación ni evidencias sobre cómo se protege la información de los sistemas durante las pruebas de auditoría. No se identifican numerales específicos en la Guía de Seguridad y Privacidad de la Información (2310200-GS-013) que desarrollen este control de manera explícita.	Para esto es importante definir un procedimiento formal para la ejecución de pruebas de auditoría, contemplando alcance, niveles de acceso, medidas de seguridad de los dispositivos, registro de accesos y eliminación segura de archivos generados. Asimismo, se sugiere incorporar estos lineamientos en la guía o en un anexo técnico, garantizando trazabilidad y protección de la información institucional.

Actividad de Control 2 – Planificación:

En la vigencia 2024 la OCI en el informe de auditoría mencionó:

"*De acuerdo con el documento maestro, para esta instancia y derivado de los resultados obtenidos en la fase de diagnóstico, se debe proceder con la elaboración del Plan de Seguridad y Privacidad de la Información. Respecto a esto, la Secretaría en la vigencia 2020 oficializó en el portal del SIG el documento PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN - PESI versión 1 Código 2310200-PL-012 el cual tiene como objetivo "Definir una estrategia de Seguridad de la información, en adelante PESI, liderada por el área de Tecnologías de Información y Comunicación - TIC, a partir de la vigencia 2020-2024 que responda a las necesidades de preservar la confidencialidad, la integridad y la disponibilidad sobre los activos de información*". Con el documento mencionado, se cumple a lo definido en esta etapa.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Para la vigencia 2025, y de acuerdo con el lineamiento del documento maestro MSPI, al realizar seguimiento se informa que de acuerdo con la información reportada por la entidad y el documento **Código 2310200-PL-012, Versión 2, Plan Estratégico de Seguridad de la Información (PESI)**, con fecha de vigencia 19-11-2024 y oficializado en SMART, se valida su actualización.

También, en este documento en el numeral 8.3 Definición de las actividades del plan operacional de seguridad y privacidad de la información, se definen actividades que se deben ejecutar anualmente, por tanto, para la vigencia 2025, se presenta el siguiente reporte de avance de acuerdo con seguimiento realizado con la OTIC así:

ITEM	Actividad	Seguimiento 2025
Activos	Levantamiento de activos de información.	Se ejecutó el levantamiento de activos de información durante la vigencia 2025, ejercicio en el cual la OTIC brindó acompañamiento a las diferentes dependencias de la entidad para consolidar el inventario institucional.
	Publicación de activos de información.	La publicación oficial de los activos de información se encuentra pendiente de aprobación y divulgación.
	Registro de activos de información, Ley 1712.	En concordancia con la actividad 1, la OTIC acompañó el proceso de actualización de activos de información para 2025.
Incidentes	Gestionar los incidentes identificados.	El ingeniero responsable del MSPI lleva una bitácora institucional para el registro de incidentes o eventos de seguridad de la información, identificándose 17 registros activos a la fecha.
	Informar las novedades de los boletines del CSIRT	Se constató que el oficial de seguridad remite a través de correo electrónico los boletines y alertas de seguridad emitidos por el COLCERT al grupo de infraestructura, contribuyendo a la gestión preventiva frente a riesgos tecnológicos.
Plan de cambio y cultura	Consejos de Seguridad.	La entidad ha desarrollado acciones de sensibilización y divulgación orientadas a fortalecer la cultura de seguridad de la información. Se destacan piezas gráficas publicadas a través del boletín interno institucional, como la campaña “Evite ser víctima de phishing”, difundida el 1 de julio de 2025, y el “Decálogo de seguridad de la información”, dispuesto en las pantallas de los equipos institucionales.
	Socializaciones en temas a la vanguardia y seguridad de la información.	Se realizaron jornadas de capacitación y sensibilización, entre ellas la “Jornada de sensibilización en seguridad digital”, llevada a cabo el 10 de junio de 2025.
MSPI	Diagnóstico de seguridad de la información.	Se verificó el diligenciamiento del instrumento de diagnóstico MSPI (objeto de la presente auditoría) por parte de la OTIC, evidenciando avances en la identificación de brechas de seguridad
	Informar diagnóstico de seguridad de la información.	El informe de diagnóstico correspondiente aún se encuentra pendiente de emisión y comunicación formal a la Alta Dirección
	Actualización documental.	En materia documental, se observó la actualización del procedimiento de gestión de vulnerabilidades y el avance en los procesos de publicación del procedimiento de gestión de accesos y administración de usuarios, así como la actualización de la guía de seguridad de la información, actualmente en trámite.
	Auditoría interna.	La Oficina de Control Interno adelanta proceso de auditoría interna al Modelo de Seguridad y Privacidad de la Información, con el propósito de evaluar la eficacia de los controles y el cumplimiento de los lineamientos técnicos establecidos por el MINTIC.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Datos personales	Solicitud bases de datos que contienen datos personales.	La OTIC solicitó a las dependencias el reporte de bases de datos que contienen información personal, con el fin de mantener actualizado el registro ante la Superintendencia de Industria y Comercio (SIC). Para la vigencia 2025 se identificaron 31 bases de datos institucionales
	Inscripción o actualización del RNBD	Las 31 bases de datos institucionales identificadas cuales fueron reportadas ante la SIC el 31 de marzo de 2025, de lo cual se evidencia certificado válido hasta marzo de 2026.
	Actualización de documentación.	Se actualizó el normograma institucional y se encuentra en trámite la actualización del procedimiento 2310200-PR-128 "Atención de requerimientos de datos personales", con el fin de armonizarlo con las disposiciones vigentes sobre protección de datos y tratamiento responsable de la información personal.

Para fortalecer este aspecto y derivado del seguimiento al plan operacional del PESI, se recomienda dar continuidad a la implementación, monitoreo y documentación de las acciones contempladas, con el fin de garantizar el cumplimiento efectivo de los objetivos estratégicos de seguridad de la información para el periodo 2024 – 2028.

Continuando con lo estipulado por el documento maestro MSPI, se indica que para esta fase se deben generar los siguientes documentos a los cuales se les realiza seguimiento así:

Requerimiento	Seguimiento OCI
Alcance MSPI	El PESI define expresamente en el numeral 4 el alcance del Modelo de Seguridad y Privacidad de la Información: "La Secretaría Jurídica Distrital adopta, establece, implementa, opera, verifica y mejora el Modelo de Seguridad y Privacidad de la Información para todos sus procesos."
Acto administrativo con las funciones de seguridad y privacidad de la información.	Dentro de la documentación entregada por la dependencia responsable, se evidencia la Resolución N.° 174 de 2021, mediante la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC al interior de la Secretaría Jurídica Distrital. De manera complementaria y de especial relevancia, en el artículo 4 de la citada resolución se adopta la "Guía de Implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC", documento que desarrolla los lineamientos y controles institucionales para preservar la confidencialidad, integridad, disponibilidad y privacidad de la información. Para la vigencia 2025, se verifica que la citada resolución y su guía continúan vigentes y aplicables, manteniendo la estructura de gobierno y las directrices institucionales en materia de seguridad y privacidad de la información. En consecuencia, este aspecto conserva su estado de cumplimiento, no siendo requerida acción adicional distinta al seguimiento a su aplicación y actualización periódica conforme a las disposiciones del Modelo de Seguridad y Privacidad de la Información – MSPI.
Adoptar la Política de Seguridad y Privacidad de la Información mediante acto administrativo, indicando el número de resolución o acto administrativo correspondiente.	Se evidencia la Resolución N.° 174 de 2021, mediante la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC.
Documento de roles y responsabilidades asociadas a la seguridad y privacidad de la información.	Durante la vigencia 2025, se observa que se encuentra en trámite interno la designación del Oficial de Seguridad de la Información, en concordancia con las características establecidas en el Modelo de Seguridad y Privacidad de la Información – MSPI y en atención del plan de mejoramiento derivado del este aspecto el año anterior. Este avance evidencia la intención institucional de formalizar la delegación de responsabilidades conforme a los lineamientos del MINTIC, los cuales establecen que esta función debe recaer en un área estratégica distinta a la Oficina de Tecnologías de la Información.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Requerimiento	Seguimiento OCI
	No obstante, a la fecha del seguimiento no se cuenta con el acto administrativo de designación, ni con el documento formal de roles y responsabilidades asociadas a la seguridad y privacidad de la información. En este sentido, el proceso se encuentra en trámite, manteniéndose el cumplimiento en desarrollo hasta la expedición del acto correspondiente y la documentación soporte.
Procedimiento de inventario y clasificación de la información e infraestructura crítica.	En 2024 la OCI indicó: "*En la entidad se cuenta con el procedimiento registro de activos de información e índice de información clasificada y reservada código 2310200-PR-025, el cual tiene como propósito "Mantener actualizado el Registro de activos de información y el Índice de Información clasificada y reservada de la Secretaría Jurídica Distrital, con base en la definición realizada por cada gestor de activos y el responsable del proceso o jefe de dependencia, a fin de verificar y mantener los niveles de protección requeridos". No obstante a lo mencionado y como oportunidad de mejora, se informa que el procedimiento no aborda el tema puntal de infraestructura crítica, por tanto, se sugiere realizar el análisis de la normatividad existente frente al tema, para incluir lo requerido respecto al tema en mención y adicionalmente, establecer estrategias que blinden la infraestructura identificada".* Ante lo descrito y realizando seguimiento para la presente vigencia se identifica que el procedimiento no ha sido actualizado para incluir el tema de infraestructura crítica.
Metodología de inventario y clasificación de la información e infraestructura crítica.	La metodología de inventario y clasificación de la información se encuentra descrita en el procedimiento mencionado en el ítem anterior.
Política de Gestión de Riesgos de la entidad, incluyendo lineamientos para la gestión de riesgos de seguridad y privacidad de la información y demás documentación asociada que determinan dichos lineamientos para la administración y gestión del riesgo.	Se verifica la existencia del documento "Política de Administración de Riesgos" (Código 2310100-OT-004, Versión 4, vigente desde el 01/08/2024), el cual define los lineamientos para la identificación, valoración y tratamiento de riesgos, incluyendo los de seguridad y privacidad de la información.
Plan de tratamiento de riesgos de seguridad de la información.	En el vínculo https://www.secretariajuridica.gov.co/node/4170 la entidad publicó para 2025 el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
Declaración de aplicabilidad.	Se encuentra publicada en SMART con 110 controles aplicables para la entidad.
Manual de políticas de Seguridad de la Información.	Se confirma la publicación en SMART de la "Guía de Implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC", documento que desarrolla los lineamientos y controles para la aplicación de la política institucional adoptada mediante la Resolución 174 de 2021. Durante la vigencia 2025, la entidad se encuentra en proceso de actualización de dicha guía, con el fin de ajustarla a los nuevos requerimientos del Modelo de Seguridad y Privacidad de la Información – MSPI y a la normatividad vigente en materia de seguridad digital.
Plan de Cambio, Cultura y Apropiación.	La OTIC dentro del repositorio de información del modelo remite el documento titulado Estrategia de Divulgación y Sensibilización de la Seguridad de la Información 2025, el cual tiene como objetivo : "*Sensibilizar a todos los integrantes de la Secretaría Jurídica Distrital, sobre la importancia de crear el hábito permanente de salvaguardar la información, con el fin de consolidar una cultura institucional de seguridad y privacidad de la información."*

Actividad de Control 3 – Operación:

En el marco del seguimiento al Modelo de Seguridad y Privacidad de la Información (MSPI), la Oficina de Control Interno realiza la validación correspondiente a la Fase 2 – Operación, la cual contempla la implementación de los procesos de seguridad de la información

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

relacionados con la gestión de activos, riesgos, incidentes, vulnerabilidades, tratamiento y evaluación de controles.

Durante esta fase, la OCI verifica la existencia, actualización y aplicación de los documentos exigidos, tales como el inventario de información, la matriz de riesgos, el plan de implementación de controles, la gestión de eventos e incidentes, la gestión de vulnerabilidades y la evidencia de la implementación de los controles de seguridad de la información, con el propósito de constatar el avance del MSPI y su alineación con el Sistema de Gestión de Seguridad de la Información (SGSI).

El instrumento MSPI indica que se deben generar los siguientes documentos:

- **Actualización del inventario de información.** Durante la vigencia 2025 se realizó la actualización del inventario de información de la entidad, en cumplimiento de la programación de este aspecto. No obstante, el instrumento se encuentra pendiente de consolidación y publicación oficial.
- **Actualización de la matriz de riesgos de seguridad de la información**. Se evidencia la actualización de la matriz de riesgos de seguridad de la información para la vigencia 2025, incorporando los resultados del autodiagnóstico MSPI y los nuevos escenarios identificados en los procesos misionales y de apoyo.
- **Plan de implementación de controles de seguridad.** La OTIC remite Plan de implementación de controles para la vigencia 2025 el cual detalla entre otros: Riesgos, Tipo de Riesgo, Naturaleza del Control, Actividad Específica, Control 27001-2022, Responsables, Fecha de inicio y Fecha Final Evidencia.
- **Actualización de la gestión de eventos e incidentes de seguridad de la información**. Se constata la existencia de una bitácora actualizada de eventos e incidentes de seguridad de la información, administrada por la Oficina TIC, donde se registran los casos reportados, su análisis y tratamiento.
- **Actualización de la gestión de vulnerabilidades**. Se evidencia la existencia de documentos técnicos elaborados por la Oficina TIC que registran los resultados de la evaluación de vulnerabilidades a los sistemas de información de la entidad, con sus respectivos reportes y acciones correctivas.
- **Evidencia de la implementación de los controles de seguridad de la información**. Se identifican avances parciales en la implementación de los controles de seguridad de la información, de acuerdo con los resultados del instrumento de evaluación del Modelo de Seguridad y Privacidad de la Información – MSPI. Algunos controles se encuentran implementados, mientras otros permanecen en fase de fortalecimiento.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Posteriormente, el instrumento MSPI para esta fase se subdivide en 3 elementos así:

NUM	DESCRIPCIÓN	REQUISITOS	NIVEL DE CUMPLIMIENTO O ANEXO A ISO 27001	Seguimiento OCI
8.1	Planificación y control operacional	Planificar, implementar, controlar & documentar el proceso del SGSI para gestionar los riesgos (i.e. un plan de tratamiento de riesgos)	40	El proceso obtiene una calificación de 40 en el instrumento de evaluación del MSPI. Como evidencia se reporta el uso del Sistema SMART para el seguimiento y control de las actividades relacionadas con la gestión de seguridad de la información; sin embargo, no se especifican los documentos o registros que soportan de manera directa el cumplimiento del requisito. *Aunque el instrumento no refleja brechas formales, se observa que la Oficina TIC no reportó información suficiente que permita identificar los aspectos o acciones específicas que deben fortalecerse para garantizar la trazabilidad y efectividad del control operacional.*
8.2	Evaluación de riesgos de seguridad de la información	(Re)hacer la apreciación y documentar los riesgos de seguridad de la información en forma regular y ante cambios o modificaciones	40	Este componente registra una calificación de 40 en el instrumento MSPI. No se evidencia documentación que respalde la actualización o reevaluación periódica de los riesgos de seguridad de la información, ni los resultados derivados de estos ejercicios frente a los cambios en los procesos o sistemas. *Si bien no se consignan brechas en el instrumento, se advierte que la Oficina TIC no suministró información adicional que permita identificar los elementos faltantes o las oportunidades de mejora requeridas para alcanzar un nivel de cumplimiento superior.*
8.3	Tratamiento del riesgo de seguridad de la información	Implementar el plan de tratamiento de riesgos (tratar los riesgos) y documentar los resultados	40	El proceso presenta una calificación de 40 en el instrumento MSPI. Para este aspecto, no se diligencia los campos evidencia y brecha, por tanto, dificulta determinar la gestión realizada y los temas que estarían pendientes en el marco de este criterio. No obstante, a lo informado, en SMART el proceso gestión TIC cuenta con la Guía de Tratamiento de Riesgos de Seguridad de la Información la cual contiene las actividades desarrollar, adicional dentro de los riesgos de gestión del proceso, se tienen contemplados 3 riesgos de seguridad de la información a los cuales se les hace seguimiento cuatrimestralmente así: • Posibilidad de afectación reputacional, por revelación o utilización de manera inadecuada de la información confidencial de la entidad. • Posibilidad de afectación reputacional, por ausencia de mecanismos de seguridad que faciliten el acceso no autorizado mediante ataques internos o externos. • Posibilidad de afectación reputacional, por afectación de forma fraudulenta a la integridad de la información de la entidad.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Actividad de Control 4 – Evaluación del desempeño:

Una vez culminadas las actividades correspondientes a la fase de operación del Modelo de Seguridad y Privacidad de la Información (MSPI versión 2025), la Oficina de Control Interno realiza la evaluación de la efectividad de las acciones implementadas, tomando como referencia los indicadores definidos en la fase de implementación.

Este seguimiento busca verificar la adecuada interacción entre el MSPI, el Modelo Integrado de Planeación y Gestión (MIPG) y el cumplimiento de los requerimientos establecidos en la Ley 1581 de 2012 sobre protección de datos personales, la Ley 1712 de 2014 de transparencia y acceso a la información pública, el Decreto 2106 de 2019, así como las demás disposiciones normativas que las reglamenten, adicionen, modifiquen o deroguen.

Los siguientes son los elementos que componen esta fase:

numeral	descripción	Calificación OTIC ANEXO A ISO 27001	SEGUIMIENTO OCI
9.1	Seguimiento, medición, análisis y evaluación	40	El proceso registra una calificación de 40 en el instrumento MSPI. Se reporta como evidencia el uso del Sistema SMART para el seguimiento institucional y la gestión de información relacionada con el SGSI; sin embargo, no se identifican los documentos o registros específicos que soporten las actividades de medición, análisis y evaluación de los controles implementados, lo cual impide evidenciar la efectividad de las acciones ejecutadas. Aunque el instrumento no presenta brechas reportadas, se recomienda diligenciar de manera completa el instrumento MSPI, identificando los documentos que soportan el cumplimiento del requisito (por ejemplo, reportes de seguimiento, indicadores de gestión, informes de desempeño o análisis de resultados) y describiendo las acciones faltantes en el campo de brechas, con el fin de mejorar la trazabilidad y control del desempeño del SGSI.
9.2	Auditoría interna	60	El componente obtiene una calificación de 60 en el instrumento MSPI. Se evidencia que el proceso de auditoría interna es desarrollado por la Oficina de Control Interno (OCI) conforme al plan anual de auditoría, el cual incluye dentro de su alcance la evaluación del Modelo de Seguridad y Privacidad de la Información – MSPI. Durante las vigencias 2024 y 2025, la OCI ha incorporado en sus planes anuales de auditoría actividades de evaluación específicas al MSPI, lo que demuestra un seguimiento sostenido y articulado con los objetivos del SGSI. En este sentido, se sugiere revalidar la calificación asignada (60) en el instrumento, considerando la evidencia de ejecución de auditorías y los resultados documentados. Aunque el instrumento no reporta brechas, se recomienda complementar su diligenciamiento identificando los documentos que soportan el cumplimiento del requisito (informes de auditoría, planes de mejoramiento, actas de seguimiento) y describir los aspectos pendientes o de mejora en el campo de brechas, con el fin de fortalecer la trazabilidad y el control del proceso de auditoría interna.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

9.3	Revisión por la dirección	40	El proceso presenta una calificación de 40 en el instrumento MSPI. No se evidencia documentación formal que demuestre la revisión periódica de la alta dirección sobre el desempeño, objetivos y eficacia del SGSI, ni los temas que podrían afectar su continuidad o efectividad. Dado que el instrumento no consigna brechas y no se cuenta con información complementaria de la OTIC, se recomienda fortalecer el diligenciamiento del instrumento MSPI, incluyendo la referencia a los documentos que evidencien la revisión por la dirección, así como también la identificación de los temas faltantes (brechas), todo esto en pro de la gestión y mejora continua del SGSI.

Actividad de Control 5 – Mejoramiento continuo:

Validar las actividades adelantadas respecto al plan de mejoramiento continuo de seguridad y privacidad de la información el cual hace parte del modelo.

NUMERAL	DESCRIPCIÓN	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	Seguimiento OCI
10.1	Mejora continua	40	El proceso presenta una calificación de 40 en el instrumento MSPI. No se evidencia documentación que soporte las acciones de mejora continua del SGSI, ni tampoco se diligencia los temas pendientes (campo brechas). Se recomienda completar el diligenciamiento del instrumento MSPI, teniendo en cuenta que para el modelo se han realizado ejercicios de auditoria interna por parte de la OCI, derivando en planes de mejoramiento, así como también identificando y relacionando documentos que evidencien la aplicación del ciclo de mejora continua , con el fin de reflejar de manera más precisa el nivel real de avance del criterio.
10.2	No conformidad y acciones correctivas	40	Este componente obtiene una calificación de 40 en el instrumento MSPI. No se evidencia documentación que registre la identificación, análisis o tratamiento de no conformidades relacionadas con la seguridad y privacidad de la información, ni las acciones correctivas adoptadas para evitar su recurrencia. Aunque el instrumento no consigna brechas, se advierte la necesidad de fortalecer el registro y trazabilidad de las acciones correctivas derivadas de las auditorías, incidentes o revisiones internas. Se recomienda diligenciar de forma completa el instrumento MSPI, referenciando los documentos o registros que soportan la atención de no conformidades (actas de comité, reportes de auditoría, planes de mejoramiento, informes de seguimiento) y describiendo en el campo de brechas las acciones pendientes o las oportunidades de mejora detectadas, de modo que se consolide la evidencia del proceso de mejora continua dentro del SGSI.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

7. FORTALEZAS

- Se observa que con base en las conclusiones de la auditoría interna realizada por la Oficina de Control Interno en 2024 al Modelo de Seguridad y Privacidad de la Información (MSPI versión 2021), la entidad a través de la Oficina de Tecnologías de la Información y las Comunicaciones desarrolló y ejecutó acciones asociadas a los planes de mejoramiento, orientadas a atender las no conformidades y observaciones señaladas en el informe anterior.

- Se evidencia voluntad institucional y compromiso de la OTIC (líder de la implementación del modelo en la entidad) para mantener la continuidad en la gestión del MSPI, principalmente debido a la actualización normativa que se suscitó en la presente vigencia.

- La entidad ha mantenido la vigencia y aplicación de la Política de Seguridad y Privacidad de la Información por medio de la guía de implementación de la política de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios TIC la cual se adoptó con la resolución interna 174 de 2021, de manera transversal a las operaciones que se realizan sobre la plataforma tecnológica de la Secretaría.

- En la vigencia 2025 se evidencia un avance positivo en la gestión de incidentes y eventos de seguridad de la información, reflejado en un mayor registro y catalogación; esto derivado del informe de auditoría al MSPI de la vigencia 2024. Este progreso demuestra el fortalecimiento de los mecanismos de trazabilidad y seguimiento dentro del Modelo, contribuyendo a la mejora continua.

- Existen avances en la identificación y tratamiento de vulnerabilidades en los sistemas de información, documentados por la OTIC.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

8. OPORTUNIDAD DE MEJORA

1. Falta de alineación y actualización de la Guía de Implementación de la Política de Seguridad y Privacidad de la Información respecto a la normatividad vigente.

La guía de implementación de la política de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios tic oficial versión 1 con fecha 01/09/2021, adoptada con la resolución interna 174 de 2021, se encuentra en proceso de revisión conjunta en la entidad, ya que su versión actual no incorpora los ajustes requeridos por los lineamientos más recientes del MINTIC asociado al Modelo de Seguridad y Privacidad de la Información MSPI.

Esta situación apunta a la alineación normativa y técnica frente a los nuevos requerimientos del modelo, lo cual podría generar riesgos asociados principalmente a la desactualización de controles de seguridad de la información, asimismo, existe el riesgo de desactualización, afectando la capacidad de la entidad para garantizar la confidencialidad, integridad, disponibilidad y trazabilidad de la información.

Por lo anterior se sugiere priorizar la actualización de la guía, incorporando los cambios en materia normativa, ya que contribuye significativamente al fortalecimiento del cumplimiento del MSPI, así como a la armonización de las buenas prácticas.

9. NO CONFORMIDADES

1. Incumplimiento de requisitos contemplados en el Modelo de Seguridad y Privacidad de la Información - MSPI

Una de las primeras actividades a ejecutar en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) consiste en la identificación de la línea base de seguridad; para tal fin se realiza un levantamiento de información, el cual sirve como insumo fundamental para el desarrollo de las fases posteriores del modelo.

El instrumento MSPI contempla un total de 42 ítems que durante el ejercicio de auditoría se identificó incumplimiento o cumplimiento parcial de los siguientes:

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Ítem	Estado de cumplimiento	Versión MSPI
Documento con el resultado de la estratificación de la entidad, aceptado y aprobado por la alta dirección.	No cumple	2021
Procedimientos de control documental del MSPI.	Parcial	2021
Inventario de partes externas o terceros a los que se transfiere información de la entidad.	No cumple	2021
Formato de acuerdo de transferencia de información.	No cumple	2021
Inventario de proveedores que tengan acceso a los activos de información, indicando el servicio que prestan o bienes que venden.	No cumple	2021
Documento con el plan de seguimiento, evaluación, análisis y resultados del MSPI, revisado y aprobado por la alta Dirección.	No cumple	2021

La anterior tabla refleja que varios de los incumplimientos y cumplimientos parciales corresponden a requisitos bajo la versión 2021 del MSPI (informados en la auditoría de la vigencia 2024), lo que evidencia brechas previas a la actualización del modelo. Estos resultados muestran que lo informado no deriva únicamente de la transición normativa, por lo que se requiere fortalecer los mecanismos de seguimiento y articulación para avanzar de manera consistente en el cumplimiento del modelo.

Complementariamente, durante el desarrollo de la auditoría se evidenció incumplimiento en aspectos asociados a la evaluación de la efectividad de los controles establecidos en el Anexo A de la norma ISO/IEC 27001:2022 que estructuran la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI). A continuación, se detallan los ítems validados:

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2022 ANEXO A

Como resultado de total se presenta una calificación de **42**, catalogándose en el nivel de madurez **Efectivo.** Los siguientes son los ítems identificados como incumplidos o con cumplimiento parcial:

Controles Organizacionales:

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Ítem	Estado de cumplimiento	Versión MSPI
Roles y responsabilidades de seguridad de la información	Incumplido	2021
Contacto con las autoridades	Parcial	2021
Contacto con grupos de interés	Parcial	2021
Inteligencia de amenazas	Incumplido	2025
Seguridad de la información en la gestión de proyectos	Incumplido	2021
Inventario de información y otros activos asociados	Parcial	2025
Uso aceptable de la información y otros activos asociados	Parcial	2021
Devolución de Activos	Parcial	2021
Etiquetado de la información	Parcial	2021
Transferencia de información	Incumplido	2021
Control de acceso	Parcial	2021
Información de autenticación	Parcial	2021
Derechos de acceso	Parcial	2025
Seguimiento, Revisión y Gestión de Cambios de Servicios de Proveedores	Parcial	2025
Seguridad de la información para el uso de servicios en la nube	Parcial	2025
Evaluación y Decisión sobre Eventos de Seguridad de la Información	Parcial	2021
Respuesta a los Incidentes de Seguridad de la Información	Parcial	2021
Aprendizaje sobre los incidentes de seguridad de la información	Parcial	2021
Recopilación de pruebas	Parcial	2021
Seguridad de la información durante la interrupción	Incumplido	2025
Preparación de las TIC para la continuidad del negocio	Parcial	2025
Protección de registros	Parcial	2021
Procedimientos operativos documentados	Parcial	2025

Controles tecnológicos:

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Ítem	Estado de cumplimiento	Versión MSPI
Eliminación de información	Incumplido	2021
Enmascaramiento de datos	Incumplido	2025
Prevención de fuga de datos	Parcial	2025
Redundancia de las instalaciones de procesamiento de información	Parcial	2021
Registro	Parcial	2021
Actividades de seguimiento	Parcial	2025
Sincronización del reloj (clock)	Parcial	2021
Filtrado web	Incumplido	2021
Uso de criptografía	Incumplido	2021
Ciclo de vida de desarrollo seguro	Parcial	2021
Requisitos de seguridad de la aplicación	Parcial	2021
Arquitectura del sistema seguro y principios de ingeniería	Parcial	2025
Codificación segura	Incumplido	2021
Pruebas de seguridad en desarrollo y aceptación	Incumplido	2021
Desarrollo subcontratado	Incumplido	2021
Separación de los entornos de desarrollo, prueba y producción	Parcial	2021

Finalmente, en revisión del instrumento de evaluación del Modelo de Seguridad y Privacidad de la Información – MSPI (el cual lleva en vigencia desde el mes de junio) correspondiente a la vigencia 2025, se evidenció que en varios numerales el diligenciamiento de los campos **evidencia y brechas** es incompleto o carece de información suficiente para verificar el cumplimiento real de los requisitos. En diferentes apartados se registran calificaciones bajas (40 o 60 puntos) sin que se relacione de forma clara la evidencia documental que respalde dichos resultados, y en otros casos no se consignan brechas o acciones pendientes.

Estas condiciones se relacionan con la normatividad y los lineamientos vinculados al Modelo de Seguridad y Privacidad de la Información del MINTIC (Resolución 500 de 2021 y Resolución 02277 de 2025), que establecen la aplicación del instrumento como herramienta base para la autoevaluación y seguimiento institucional del MSPI. Asimismo, se aparta de lo dispuesto en la Política Institucional de Seguridad y Privacidad de la Información adoptada mediante Resolución 174 de 2021, la cual establece la responsabilidad de propender por la continuidad de la operación de los servicios y dar

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

cumplimiento a los requisitos legales, reglamentarios y regulatorios, Orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información.

Lo anterior apunta a riesgos de incumplimientos normativos y de afectación a los pilares de seguridad de la información integridad, disponibilidad y confidencialidad.

Finalmente se indica que la Oficina de Control Interno aclara que el ejercicio auditor sobre el Modelo de Seguridad y Privacidad de la Información - MSPI se realizó con base en la normatividad vigente para la vigencia 2025, la cual incluye las actualizaciones introducidas a raíz de los ajustes derivados y la actualización de la versión más reciente de la norma ISO 27001, así como también la actualización de los documentos asociados descritos en la resolución 02277 de 2025.

10. RECOMENDACIONES

- Establecer acciones por parte de líder de la implementación del modelo en la entidad con el fin de garantizar la obtención completa de los 42 ítems de levantamiento de información del instrumento MSPI, asegurando que cada numeral cuente con evidencias actualizadas, verificables y aprobadas. De manera complementaria, incluir dentro del PESI la definición del plan de implementación.

- Diligenciar por parte de la OTIC de manera completa y verificable la nueva versión del instrumento MSPI, asegurando que cada calificación esté acompañada de las evidencias documentales que respalden el cumplimiento del requisito, y que en el campo de brechas se describan de forma clara las acciones faltantes, oportunidades de mejora o documentos por actualizar. Igualmente, se sugiere establecer un mecanismo de revisión y validación interna del instrumento de manera periódica, para ir realizando medición del avance o grado de madurez del modelo, garantizando la coherencia entre la información registrada, los resultados y la realidad institucional del MSPI.

- Se recomienda a la entidad fortalecer la gestión documental y de evidencias del Modelo de Seguridad y Privacidad de la Información – MSPI, implementando una estructura organizada y estandarizada del repositorio institucional, que permita la fácil identificación, acceso y trazabilidad de los documentos conforme a los numerales y componentes definidos en el modelo.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

El líder del MSPI en la entidad deberá gestionar este aspecto, garantizando que toda la información que sea completa, vigente, verificable y coherente con lo dispuesto en la documentación de la modelo dispuesta por MINTIC, particularmente con el compromiso institucional de proteger, preservar y administrar la confidencialidad, integridad, disponibilidad de la información.

Asimismo, se recomienda establecer mecanismos de control documental y validación periódica de evidencias, definiendo responsables, procedimientos y frecuencias de revisión que aseguren la actualización continua de los soportes.

- Se recomienda al responsable de la implementación del Modelo de Seguridad y Privacidad de la Información realizar un análisis integral de la gestión de riesgos de seguridad de la información y generar los lineamientos necesarios para que en la entidad se identifiquen las posibles brechas, vulnerabilidades o eventos no controlados que puedan afectar los activos de información institucionales. Dicho análisis debe derivar en la actualización de las fuentes de información que sustentan la gestión de riesgos, principalmente el registro de eventos e incidentes de seguridad de la información, asegurando que estos se encuentren debidamente documentados, analizados y gestionados conforme a las situaciones reales identificadas.

11. CONCLUSIONES

Se observan avances en la gestión institucional frente a las observaciones formuladas en la vigencia 2024, destacándose la ejecución de acciones de mejoramiento orientadas al cumplimiento de los lineamientos del MINTIC y al fortalecimiento del sistema de gestión de seguridad de la información en la Secretaría. La Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) ha mantenido un compromiso constante con la continuidad del modelo, reflejado en la actualización de la documentación, el seguimiento de eventos e incidentes de seguridad y el tratamiento de vulnerabilidades en los sistemas de información.

No obstante, se identificaron aspectos que requieren atención prioritaria, principalmente relacionados con la aplicación de las herramientas de diagnóstico y autoevaluación del MSPI el cual se formalizó en el mes de junio de la presente vigencia por parte de MINTIC, en actividades tales como consolidación y levantamiento de las evidencias que los sustentan, situaciones que afectan la trazabilidad, la verificación objetiva del cumplimiento y la medición del nivel de madurez del modelo, representando riesgos para la evaluación integral del desempeño institucional en materia de seguridad y privacidad de la información.

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Finalmente, aunque la calificación global obtenida refleja la necesidad de continuar con el fortalecimiento del modelo, se reconoce el avance institucional en la gestión técnica y documental, así como la voluntad de mejora continua evidenciada por la OTIC. La implementación de las recomendaciones propuestas contribuirá al incremento del nivel de madurez del MSPI, al cumplimiento del marco normativo vigente y al aseguramiento progresivo de los principios de confidencialidad, integridad y disponibilidad de la información institucional.

Original Firmado
DIEGO ALEXANDER URAZAN FRANCO
Firma Auditor Líder

Original Firmado
OLGA MILENA CORZO ESTEPA
Firma Jefe Oficina de Control Interno

Carrera 8 No. 10 – 65
Código Postal: 111711
Tel: 3813000
www.bogotajuridica.gov.co
Info: Línea 195

Bogotá, D.C. 7 de noviembre de 2025

Ingeniero:
OSCAR JAVIER SUAREZ
Oficina de Tecnología de la Información y Comunicación
SECRETARIA JURÍDICA DISTRITAL

Asunto: Resultado a las respuestas brindadas al informe preliminar de auditoría al Modelo de Seguridad y Privacidad de la información - MSPI - ISO 27001

Respetado Ingeniero,

Analizadas las respuestas brindadas por la Oficina de Tecnología de la Información y Comunicación al informe preliminar de auditoría al Modelo de Seguridad y Privacidad de la información - MSPI - ISO 27001 comunicadas mediante correo electrónico del 6 de noviembre de 2025, la Oficina de Control Interno informa:

Ítem dentro del informe.	Detalle del resultado preliminar	Respuesta OTIC	Análisis y conclusión, Oficina de Control Interno
6.2. ACTIVIDADES DE AUDITORÍA BASADA EN RIESGOS – ANÁLISIS POR ACTIVIDADES DE CONTROL..	Durante la vigencia 2025, el equipo auditor de la Oficina de Control Interno desarrolló la evaluación al Modelo de Seguridad y Privacidad de la Información – MSPI, en el marco de las disposiciones actualizadas por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, particularmente lo establecido en la Resolución 2277 de 2025, la cual actualiza el Anexo 1 de la Resolución 500 de 2021 y fortalece los lineamientos asociados a la gestión de la seguridad digital y la protección de la información.	Conforme a las observaciones presentadas en la mesa de trabajo, es necesario precisar que la actualización del MSPI se materializó por parte de MinTIC en junio de 2025, evaluar la implementación de la actualización en septiembre de la misma vigencia solo permite trazar una línea base…. Adicionalmente, se llama la atención en cuanto a que, formalmente en la SJD se tiene únicamente la resolución de adopción del Modelo MSPI versión 2021….	El comentario de la OTIC sobre el tiempo limitado de implementación es válida; sin embargo, la auditoría debe mantener su evaluación frente a la normativa vigente. La Resolución 2277 de 2025 emitida por MinTIC constituye una norma nacional de obligatorio cumplimiento para todas las entidades públicas, por lo que, aun cuando la SJD cuente con resolución interna de adopción de la versión 2021, es prioritario cumplir con la versión actualizada. En consecuencia, el resultado obtenido se constituye como la línea base inicial para la transición hacia la actualización 2025. De igual manera para este párrafo se incluye que la norma entra en vigencia el 3 de junio de 2025, acogiendo el comentario de la OTIC.
6.2. ACTIVIDADES DE AUDITORÍA BASADA EN RIESGOS – ANÁLISIS POR ACTIVIDADES DE CONTROL..	El ejercicio tuvo como propósito verificar la efectividad de la gestión adelantada por la Oficina de Tecnologías de la Información y las Comunicaciones en la implementación y mejora continua del modelo, así como medir el grado de cumplimiento frente a los nuevos requerimientos normativos y técnicos establecidos para las entidades públicas.	Como indique anteriormente, la actualización del MSPI se formalizó en junio y la auditoria se desarrolla en septiembre de 2025, medir la efectividad de la gestión de cambio en tres meses es prematuro, en este sentido, se sugiere respetuosamente se indique la importancia de generar la línea base que debe atender la OTIC para la migración de la versión 2021 a 2025	En complemento a lo indicado en el ítem previo y conforme a lo manifestado por la OTIC, se considera fundamental consolidar la línea base del nuevo modelo, la cual permitirá determinar las acciones necesarias para la próxima vigencia y facilitar la construcción de un plan de mejoramiento eficaz que contribuya al fortalecimiento del nivel de madurez del MSPI.
Actividad de control 1 - Diagnóstico	En comparación con la vigencia anterior, donde la evaluación general alcanzó un 80% de cumplimiento, se observa una disminución porcentual en la calificación, atribuible principalmente a la actualización normativa y técnica introducida por la Resolución 2277 de 2025 y la adopción de la ISO27001:2022, así como también a un ejercicio detallado de evaluación y validación por parte de la OTIC.	Si bien es correcta la conclusión, es importante considerar que, el tiempo de implementación del modelo nuevo no es suficiente para medir las actividades diferentes al diagnostico	A partir de la respuesta emitida por la OTIC y de la línea base existente, se recomienda que el plan de mejoramiento incorpore acciones concretas, con plazos realistas y coherentes de acuerdo a los requisitos definidos en cada criterio del instrumento.

Actividad de control 1 - Diagnóstico	Durante la vigencia 2025, se observa un avance en la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, pasando de un 23% de avance en 2024 a un 47% en 2025, lo que refleja una mejora en la gestión y consolidación del modelo. Como se indicó, este progreso se da en el marco de la actualización normativa sobre la cual se redefinieron los criterios y dominios de evaluación, aumentando el nivel de exigencia. Los resultados reflejan una gestión en consolidación, con avances evidentes en planificación, ejecución y mejora continua, aunque persiste la necesidad de seguir fortaleciendo la medición, la documentación de evidencias y la articulación institucional para garantizar la sostenibilidad y efectividad del MSPI.	Sugiero aclarar la versión del MSPI… respetuosamente sugiero dejar constancia que los avances evidenciados se enmarcan principalmente en la versión del MSPI que se tenía vigente en el primer semestre de 2025	El proceso auditor se efectuó con fundamento en la versión 2025 del MSPI, por tanto, constituye el marco normativo vigente. Sin embargo, se presenta un comparativo con el porcentaje de cumplimiento de la vigencia pasada para facilitar la interpretación de los avances y brechas. A pesar de que el instrumento actualizado incorpora cambios y ajustes metodológicos, conserva elementos conceptuales y técnicos compatibles con la versión anterior, permitiendo establecer un contraste coherente entre ambos modelos.
Actividad de control 1 - Diagnóstico Cuadro levantamiento de información Ítem 24	Inventario de partes externas o terceros a los que se transfiere información de la entidad. No se reporta información en el instrumento MSPI. No cumple	No me queda claro el incumplimiento, salvo que, se tenga evidencia que se ha requerido la trasferencia de información por parte del dueño del activo	El tema se sustenta inicialmente en la calificación reportada y en la ausencia de información sobre evidencias que demuestren el cumplimiento del criterio en el instrumento. De igual forma, y a manera de ejemplo se menciona que según lo establecido en el Plan Estratégico de Tecnologías de la Información – PETI, la entidad mantiene relaciones con terceros a quienes se entrega información institucional, lo que debe ser documentado de manera explícita en el instrumento MSPI, ya que esto se asocia a lo descrito en el lineamiento. 
Actividad de control 1 - Diagnóstico Cuadro levantamiento de información Ítem 26	Inventario de proveedores que tengan acceso a los activos de información, indicando el servicio que prestan o bienes que venden Durante el seguimiento realizado, la OTIC informó que el Inventario de proveedores con acceso a los activos de información, indicando el servicio que prestan o los bienes que suministran, se encuentra en proceso de construcción No cumple	Solicito contrastar con la clasificación del activo de información, de conformidad con lo establecido con el dueño (responsable) del activo	De acuerdo con lo validado en trabajo de campo con el contratista encargado del MSPI, el tema se presentó debido a que el documento está en proceso de construcción, por tanto y teniendo en cuenta lo indicado en la respuesta, se sugiere adelantar las acciones que se estimen convenientes para garantizar el cumplimiento del criterio.
Actividad de control 1 - Diagnóstico Cuadro levantamiento de información Ítem 41	Documento con el plan de seguimiento, evaluación y análisis para el MSPI, revisado y aprobado por la alta Dirección. La OTIC informa que no se ha elaborado el documento con el plan de seguimiento, evaluación, análisis y resultados del Modelo de Seguridad y Privacidad de la Información (MSPI), revisado y aprobado por la Alta Dirección. No cumple	No me queda claro xq se repite, ya se había evaluado en el numeral 38	A pesar de la observación de la OTIC sobre la posible repetición del criterio, se precisan diferencias: • El **numeral 38** incluye el componente de *resultados del MSPI*, • El **numeral 41** solo contempla *seguimiento, evaluación y análisis*, lo que confirma que se trata de controles independientes dentro del instrumento. La ausencia del documento solicitado para los ítem 38 y 41 constituye una brecha frente a la Resolución 2277 de 2025, norma nacional obligatoria y prioritaria sobre la resolución interna 2021. En consecuencia, se ratifica el no cumplimiento para esos dos aspectos.
Dominio controles organizacionales	Roles y responsabilidades de seguridad de la información De acuerdo con lo establecido en el numeral 7.2.3 de la Guía, sobre roles y responsabilidades, la entidad debe designar formalmente un responsable del MSPI con un equipo de apoyo dependiente de un área estratégica distinta a la de Tecnología	Esto no es correcto, el problema es que formalmente está asignada a la OTIC, lo que no cumple con lo estipulado en el modelo 2025 del MSPI…	La respuesta de la OTIC permite evidenciar que el rol permanece adscrito a dicha oficina; sin embargo, conforme al MSPI versión 2025, establecido mediante Resolución 2277 de 2025, el Oficial de Seguridad de la Información debe ubicarse en una dependencia estratégica que garantice independencia respecto de las áreas operadoras de infraestructura tecnológica. Por lo anterior, el incumplimiento se mantiene y se recomienda continuar con la ejecución del plan de mejoramiento institucional para asegurar la reubicación del rol y el cumplimiento de la estructura definida por el modelo.

Dominio controles organizacionales	Seguridad de la información para el uso de servicios en la nube El proceso asigna una calificación de 20 puntos, indicando la ausencia de lineamientos sobre seguridad de la información en el uso de servicios en la nube Se considera pertinente establecer políticas y procedimientos que regulen el uso de estos servicios, definiendo controles de seguridad, gestión de acceso y custodia de información institucional alojada en entornos externos, lo anterior teniendo en cuenta la implementación de nube pública que actualmente está realizando al OTIC.	No es claro el alcance indicado en cuanto a establecer políticas y procedimientos que regulen el uso de la nube, sin embargo, aclaro que, todo proyecto de orden tecnológico debe estar en el PETI, entendería que se hace referencia a ello…, respetuosamente solicito confirmar	La observación inicial se formuló a partir de lo reportado por el proceso, particularmente en relación con la inexistencia de lineamientos para este criterio. No obstante, teniendo en cuenta la respuesta presentada por la OTIC, la recomendación se ajusta y complementa, indicando que, además de formular políticas y procedimientos, es indispensable cumplir con todos los elementos requeridos por el criterio según lo establecido en la documentación oficial del MinTIC.
Dominio controles de personas:	Acuerdos de confidencialidad o no divulgación Se observa que la Guía de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC contempla en el numeral 4.9.3.3 “Acuerdos de Confidencialidad o No Divulgación” la obligación de establecer, revisar y documentar los requisitos aplicables a los acuerdos de confidencialidad que garanticen la protección de la información institucional. Asimismo, se dispone que en todos los convenios o contratos suscritos por la entidad con funcionarios, contratistas y demás personal, se debe incluir una cláusula de confidencialidad y reserva de la información. Al no identificarse soportes documentales en el repositorio que acrediten el cumplimiento integral de este criterio, y considerando la calificación otorgada de 40 puntos, se recomienda adelantar las acciones necesarias para evidenciar la aplicación y trazabilidad de los acuerdos de confidencialidad en todos los contratos y vínculos vigentes, asegurando su actualización conforme a los lineamientos de la guía.	No me queda claro el contexto de este punto, en mi experiencia de ingreso, así como de las OPS que se han contratado en la OTIC, se firma un acuerdo de confidencialidad, la observación está encaminada a implementar otro acuerdo?	Conforme a la respuesta emitida por la OTIC, la observación de auditoría se origina porque la calificación asignada (40 puntos) no estuvo respaldada por evidencia documental que demostrara su cumplimiento. No obstante, se identifica que la entidad aplica controles y que la Guía de Seguridad y Privacidad de la Información incluye numerales alineados con este criterio. Por lo anterior, la recomendación se enfoca en fortalecer la información reportada en el instrumento MSPI, dado que la existencia de actividades y lineamientos amerita revalidar la calificación y reflejar de manera adecuada el nivel real de cumplimiento.
Dominio controles de personas:	Perímetros de seguridad física En seguimiento a este criterio, se evidencia que la entidad dispone de lineamientos establecidos en la Guía de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios TIC, donde se contemplan disposiciones relacionadas con el control de acceso físico, la protección de las instalaciones y la custodia de los activos tecnológicos Sin embargo, considerando la calificación otorgada de 40 puntos, se propone fortalecer la evidencia documental que soporte la aplicación de dichas medidas, especialmente las referidas a controles de ingreso, bitácoras de acceso y mecanismos de protección física en las áreas críticas.	Considero importante precisar las áreas críticas, por parte de la OTIC, el data center cuenta con el control de acceso físico, en cuanto a la custodia de los activos, considero necesario hace parte activa del análisis a los dueños o los responsables de los activos de información	Además de lo señalado por la OTIC respecto a los controles implementados en el data center, se identifica que el instrumento MSPI también registra controles institucionales adicionales, tales como lectores de tarjetas de proximidad para el ingreso a las instalaciones, uso de carné de identificación y mecanismos biométricos. En este contexto, y considerando la calificación asignada de 40 puntos, se recomienda revalidar dicho puntaje y de manera complementaria, fortalecer la evidencia y la justificación documental que respalde el cumplimiento de este criterio.

Dominio controles de personas:	Supervisión de la seguridad física Se evidencia que la entidad dispone de mecanismos de supervisión y monitoreo físico, tales como sistemas de videovigilancia, alarmas contra intrusión y controles de acceso restringido, los cuales permiten vigilar de manera continua las áreas críticas y detectar posibles eventos no autorizados. Los sistemas instalados cumplen con las disposiciones establecidas en la Guía de Seguridad y Privacidad de la Información (código 2310200-GS-013, numeral 4.7.1.3 “Supervisión de la Seguridad Física”), que orienta la implementación de medidas preventivas y reactivas para salvaguardar las instalaciones y los activos tecnológicos De acuerdo con la calificación otorgada de 60 puntos, se considera que el control se encuentra implementado y operando; no obstante, se recomienda fortalecer la evidencia documental y la justificación que respalde el cumplimiento de este criterio.	Es preciso aclarar el alcance del fortalecimiento que se recomienda, ello considerando que, por competencia tendremos que dar traslado a la DDGC quien supervisa lo relacionado con la seguridad física de la sede	De acuerdo con lo indicado por la OTIC, la recomendación de la OCI se centra en verificar la coherencia entre la calificación otorgada y los controles actualmente implementados y operativos en la entidad. Adicionalmente, las acciones orientadas al fortalecimiento del cumplimiento del criterio que demanden la intervención de otras dependencias deberán ser gestionadas internamente por la entidad; en tal sentido, se aconseja incorporarlas cuando así se requiera.
Dominio controles de personas:	Ubicación y Protección del equipo La Secretaría Jurídica Distrital cuenta con lineamientos establecidos en la Guía de Seguridad y Privacidad de la Información (código 2310200-GS-013), particularmente en los numerales 4.7.2 “Ubicación y Protección de Equipos” y subsiguientes, que definen medidas para la protección física y eléctrica de la infraestructura tecnológica, la seguridad del cableado, el mantenimiento preventivo y correctivo, y los procedimientos para el retiro controlado de activos. La Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) ejecuta mantenimientos conforme a un cronograma establecido, dispone de estaciones de trabajo con conexiones eléctricas reguladas y cableado protegido mediante canaletas, contribuyendo a la conservación de los activos tecnológicos. En este sentido, se valida la existencia de controles físicos y eléctricos operativos, como sistemas de protección ante fallas eléctricas y mecanismos de registro para el retiro de equipos. No obstante, considerando la calificación de 60 puntos, se recomienda fortalecer la evidencia documental y verificar la aplicación integral de los lineamientos, especialmente en lo relativo al monitoreo de condiciones ambientales, protección del cableado y mantenimiento programado, con el fin de elevar el nivel de cumplimiento y garantizar la continuidad operativa en condiciones seguras.	De acuerdo, la acción de la OTIC se concentra en el data center, los circuitos eléctricos no son atendidos por nosotros, sugiero precisar el alcance del fortalecimiento que	En atención a lo mencionado por la OTIC, se precisa que las recomendaciones emitidas por la OCI tienen un carácter orientador y general, sin que ello implique obligatoriedad en su adopción. Corresponde al dueño del proceso definir las acciones, actividades y documentación que considere necesarias para asegurar el cumplimiento del criterio. En este sentido, la OTIC tiene plena potestad para determinar las medidas que estime pertinentes.
Dominio controles tecnológicos:	Restricción de acceso a la información Se considera pertinente revisar y reevaluar la calificación, sustentándola en evidencias técnicas, registros de control y trazabilidad de accesos que permitan determinar con mayor precisión el grado real de cumplimiento. Así mismo, se sugiere fortalecer la gestión del control de accesos, mediante la verificación periódica de privilegios, y asegurar que la asignación, modificación y revocación de permisos se realicen de acuerdo con los lineamientos institucionales y las buenas prácticas de seguridad de la información establecidas en la Guía 2310200-GS-013, garantizando una protección efectiva de la información durante todo su ciclo de vida.	Me causa extrañeza esta respuesta, en la SJD no tenemos AZURE y tampoco Office 365… Adicionalmente, no me queda claro el tipo de evidencias adicionales que se consideran sustentan la calificación que la Oficina consideró, en este sentido, respetuosamente sugiero valorar el cumplimiento que se da al procedimiento indicado en el A 8.2	Con base en lo señalado por la OTIC, el comentario del informe final se ajusta conforme a lo consignado en el instrumento MSPI. Ante este aspecto, se indica que se presentó un error de copia de información desde el requisito quedando registrado dentro del seguimiento.

Dominio controles tecnológicos:	Acceso al código fuente De acuerdo con lo reportado en el seguimiento es recomendable revisar y reevaluar la calificación, sustentándola en evidencias técnicas, registros de control y trazabilidad de accesos que permitan determinar con mayor precisión el grado real de cumplimiento. Así mismo, se sugiere fortalecer la gestión del control de accesos, mediante la verificación periódica de privilegios, y asegurar que la asignación, modificación y revocación de permisos se realicen de acuerdo con los lineamientos institucionales y las buenas prácticas de seguridad de la información establecidas en la Guía 2310200-GS-013, garantizando una protección efectiva de la información durante todo su ciclo de vida.	No están implementados en la SJD	Con base en lo señalado por la OTIC, el comentario del informe final se ajusta conforme a lo consignado en el instrumento MSPI. Ante este aspecto, se indica que se presentó un error de copia de información desde el requisito quedando registrado dentro del seguimiento.
Actividad de Control 4 – Evaluación del desempeño:	Una vez culminadas las actividades correspondientes a la fase de operación del Modelo de Seguridad y Privacidad de la Información (MSPI), la Oficina de Control Interno realiza la evaluación de la efectividad de las acciones implementadas, tomando como referencia los indicadores definidos en la fase de implementación.	Considero importante indicar la versión	Se incluye la versión para el informe final.
7.FORTALEZAS	Se observa que con base en las conclusiones de la auditoría interna realizada por la Oficina de Control Interno en 2024 al Modelo de Seguridad y Privacidad de la Información (MSPI), la entidad a través de la Oficina de Tecnologías de la Información y las Comunicaciones desarrolló y ejecutó acciones asociadas a los planes de mejoramiento, orientadas a atender las no conformidades y observaciones señaladas en el informe anterior.	Versión 2021	Se incluye la versión para el informe final.
7.FORTALEZAS	La entidad ha mantenido la vigencia y aplicación de la Política de Seguridad y Privacidad de la Información por medio de la guía de implementación de la política de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios TIC de manera transversal a las operaciones que se realizan sobre la plataforma tecnológica de la Secretaría.	Sugiero complementar con la resolución con la que se adoptó el modelo en la SJD	Se incluye la Resolución Interna para el informe final.
8.OPORTUNIDAD DE MEJORA	La guía de implementación de la política de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios tic oficial versión 1 con fecha 01/09/2021 se encuentra en proceso de revisión conjunta en la entidad, ya que su versión actual no incorpora los ajustes requeridos por los lineamientos más recientes del MINTIC asociado al Modelo de Seguridad y Privacidad de la Información MSPI.	Sugiero incluir la resolución de adopción	Se mencionará la resolución Interna para el informe final.
9. NO CONFORMIDADES	1. Incumplimiento de requisitos contemplados en el Modelo de Seguridad y Privacidad de la Información - MSPI	No considero procedente generar el incumplimiento considerando que han trascurrido tres meses desde la formalización de la actualización del modelo y la verificación de cumplimiento en cuanto a la implementación por parte de la OCI, respetuosamente sugiero considerar que la implementación del modelo 2021 lleva no menos de tres años en la SJD…. Propongo que la no conformidad se circunscriba a las actividades de Diagnóstico Sugiero incluir la versión	Se aclara que la no conformidad se mantiene debido a que varios de los aspectos incumplidos corresponden a requisitos que ya exigía la versión 2021 del MSPI y que, según el nivel de avance reportado por la entidad, debían encontrarse implementados, mencionando entre otros el tema de roles, criptografía, desarrollo seguro, pruebas de seguridad de sistemas. La actualización normativa introducida en junio de 2025 permitió ampliar el alcance de la evaluación para incluir los nuevos lineamientos; sin embargo, estos no son el origen principal de las brechas evidenciadas. En consecuencia, la observación se ajusta para reflejar tanto los elementos no cumplidos del modelo anterior como los requisitos actualizados, garantizando a la OTIC una visión completa del estado del modelo y la necesidad de un plan de mejoramiento sólido.

9. NO CONFORMIDADES	Finalmente, en revisión del instrumento de evaluación del Modelo de Seguridad y Privacidad de la Información – MSPI correspondiente a la vigencia 2025, se evidenció que en varios numerales el diligenciamiento de los campos evidencia y brechas es incompleto o carece de información suficiente para verificar el cumplimiento real de los requisitos. En diferentes apartados se registran calificaciones bajas (40 o 60 puntos) sin que se relacione de forma clara la evidencia documental que respalde dichos resultados, y en otros casos no se consignan brechas o acciones pendientes.	Solicito complementar la evaluación indicando que han trascurrido tres meses desde la formalización de la actualización del nuevo MSPI	El comentario se acepta, por tanto se incluye en el informe final.
9. NO CONFORMIDADES	Estas condiciones se relacionan con la normatividad y los lineamientos vinculados al Modelo de Seguridad y Privacidad de la Información del MINTIC (Resolución 500 de 2021 y Resolución 02277 de 2025), que establecen la aplicación del instrumento como herramienta base para la autoevaluación y seguimiento institucional del MSPI. Asimismo, se aparta de lo dispuesto en la Política Institucional de Seguridad y Privacidad de la Información adoptada mediante Resolución 174 de 2021, la cual establece la responsabilidad de propender por la continuidad de la operación de los servicios y dar cumplimiento a los requisitos legales, reglamentarios y regulatorios, Orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información.	Respetuosamente sugiero revisar esta conclusión, en el mismo informe se reconoce el avance y consolidación de resultados en cuanto al cumplimiento de la versión del MSPI versión 2021…	Este párrafo hace parte de la no conformidad, donde se informa el criterio normativo que se incumple.
10. RECOMENDACIONES	Establecer acciones por parte de líder de la implementación del modelo en la entidad con el fin de garantizar la obtención completa de los 42 ítems de levantamiento de información del instrumento MSPI, asegurando que cada numeral cuente con evidencias actualizadas, verificables y aprobadas.	Sugiero ajustar por, definir el plan de implementación de la actualización del MSPI versión 2025 en el PESI	Se acepta el comentario, por tanto la recomendación será complementada.
10. RECOMENDACIONES	El líder del MSPI en la entidad deberá gestionar este aspecto, garantizando que toda la información que sea completa, vigente, verificable y coherente con lo dispuesto en la documentación de la modelo dispuesta por MINTIC, particularmente con el compromiso institucional de proteger, preservar y administrar la confidencialidad, integridad, disponibilidad de la información.	No estoy de acuerdo, la responsabilidad es de todos en la Entidad… dejar una sola persona es totalmente inviable	En el entendido de que la implementación del Modelo aplica a toda la entidad, la recomendación se orienta específicamente al control y reporte de la información en el instrumento MSPI. No obstante, se reitera que la necesidad de fortalecer los aspectos asociados a la gestión documental corresponde a un alcance institucional más amplio.
10. CONCLUSIONES	No obstante, se identificaron aspectos que requieren atención prioritaria, principalmente relacionados con la aplicación de las herramientas de diagnóstico y autoevaluación del MSPI, consolidación y levantamiento de las evidencias que los sustentan, situaciones que afectan la trazabilidad, la verificación objetiva del cumplimiento y la medición del nivel de madurez del modelo, representando riesgos para la evaluación integral del desempeño institucional en materia de seguridad y privacidad de la información.	Considero que hace falta por parte del auditor indicar que la versión actualizada del MSPI se formalizó en junio de 2025, es decir, para la Entidad es una oportunidad el iniciar con la implementación de la actualización….	Se tendrá en cuenta este comentario para el informe final; no obstante, la permanencia de la no conformidad se sustenta en que los incumplimientos identificados corresponden a requisitos que ya debían estar implementados bajo la versión 2021 del MSPI y que fueron señalados en el registro anterior.

De manera complementaria y una presentados los resultados de la auditoría en reunión de cierre y especialmente en referencia a la no conformidad, la OTIC genera los siguientes comentarios:

- Desarrollo subcontratado: El ingeniero Iam Ojeda pregunta que si este aspecto aplica para los contratos de prestación de servicios. Ante esto y en el entendido de la figura de OPS sobre la cuales se contratan servicios de ingenieros para desarrollar sobre los sistemas de información, se sugiere tenerlos en cuenta dentro de este criterio.

- Ciclo de vida de Desarrollo seguros: La ingeniera Stefany Briceño pregunta acerca de porque el incumplimiento siendo que en la entidad existe documentación en el SIG sobre este tema, así como también se ejecutan actividades relacionadas; ante esto el equipo auditor indica que precisamente y sin desconocer la existencia de la documentación asociada al proceso gestión TIC relacionado con desarrollo de software, en el instrumento MSPI se califica con 20 y el tema se asocia a que faltan los 3 ambientes estipulados en la guía de seguridad y privacidad para todos los sistemas de información, por ende se recomienda realizar revisión de este aspecto con el fin de determinar el grado real de cumplimiento.

Atentamente,

Original firmado
OLGA MILENA CORZO ESTEPA
Jefe Oficina de Control Interno

Elaborado por: *Diego Alexander Urazán Franco – Contratista.*
Revisado y Aprobado por: *Dra. Olga Milena Corzo Estepa – Jefe Oficina de Control Interno*