**MEMORANDO**

150
Bogotá D.C., 17 de diciembre de 2025

**PARA:** **Dr. GUSTAVO QUINTERO ARDILA**
Secretario Distrital de Gobierno

**DE:** **JEFE OFICINA DE CONTROL INTERNO**

**ASUNTO:** Informe Final Auditoría Interna al Modelo de Seguridad y Privacidad de la Información (MSPI)

Respetado Secretario.

De manera atenta y en cumplimiento de lo establecido en el Plan Anual de Auditoría Interna (PAAI), aprobado para la vigencia 2025, me permito remitir el informe final de la auditoría interna al Modelo de Seguridad y Privacidad de la Información (MSPI), cuyos resultados sirven como insumo para la formulación de acciones orientadas a corregir las situaciones identificadas, mitigar la ocurrencia de riesgos, fortalecer la gestión institucional y respaldar la toma de decisiones.

El presente informe se pone en conocimiento del señor Secretario, en cumplimiento de lo dispuesto en el Decreto 338 de 2019, "por el cual se modifica el Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, en lo relacionado con el Sistema de Control Interno y se crea la Red Anticorrupción", específicamente en su artículo 1, parágrafo 1, el cual establece que los informes de auditoría, seguimientos y evaluaciones tendrán como destinatario principal al representante legal de la entidad y al Comité Institucional de Coordinación de Control Interno y/o Comité de Auditoría y/o Junta Directiva, y deberán ser remitidos al nominador cuando así lo requiera.

Por lo anterior, la segunda línea de defensa, en el marco de su función de autocontrol, deberá efectuar el monitoreo y seguimiento a las observaciones derivadas de los informes emitidos por esta Oficina, con el fin de proponer acciones orientadas a aprovechar las oportunidades de mejora y adoptar las medidas necesarias frente a las recomendaciones formuladas, para el cierre de las brechas identificadas, las cuales serán objeto de verificación en cuanto a su efectiva implementación.

Finalmente, me permito informar que el informe se comunicó a la Dirección de Tecnología e Información con comunicación No. 20251500482763 del 17-12-2025 y se encuentra publicado en la página web https://www.gobiernobogota.gov.co/transparencia/planeacion-presupuesto-informes/informesoficinacontrol-interno/otros-informes-consultas-a-bases-de-datos-o-sistemas-de-informacion/informes-de auditoria

Cordialmente,

(ORIGINAL FIRMADO)
**LADY JOHANNA MEDINA MURILLO**
Jefe Oficina de Control Interno

**Anexo**: Informe Final Auditoría Interna de MSPI
**Elaboró:** Peter Vargas -Contratista OCI
**Aprobó**: Lady Johanna Medina Murillo – Jefe Oficina de Control Interno

# MEMORANDO

150

Bogotá D.C., 17 de diciembre de 2025

**PARA:** **Dr. MARIO ALEXANDER ORTIZ SALGADO**
Dirección de Tecnología e Información

**DE:** **JEFE OFICINA DE CONTROL INTERNO**

**ASUNTO:** Informe Final - Auditoría Interna al Modelo de Seguridad y Privacidad de la Información (MSPI)

Respetado Doctor Mario:

De conformidad con lo establecido en el Plan Anual de Auditoría Interna 2025 V5 y en concordancia con la implementación del Modelo de Seguridad y Privacidad de la Información por parte de la Secretaría Distrital de Gobierno, se remite como anexo el informe definitivo del proceso auditor, el cual fue socializado en reunión de cierre con la Dirección de Tecnología e Información el pasado 15 de diciembre de la presente vigencia.

Agradecemos la disposición y la atención oportuna brindada durante el desarrollo del proceso de auditoría, así como la receptividad frente a las recomendaciones formuladas, las cuales darán lugar a la suscripción de los correspondientes planes de mejoramiento derivados de los hallazgos identificados.

Cordialmente,

(ORIGINAL FIRMADO)
**LADY JOHANNA MEDINA MURILLO**
Jefe Oficina de Control Interno

**Anexo:** Informe Final Auditoría Interna MSPI

**Elaboró**: Peter Vargas – Contratista - OCI
**Aprobó**: Lady Johanna Medina Murillo – Jefe de Oficina de Control Interno

**Auditoría de Gestión**
**Modelo de Seguridad y Privacidad de la Información Nivel Central**

## I. DESTINATARIOS

- Gustavo Alberto Quintero Ardila - Secretario Distrital De Gobierno
- Mario Alexander Ortiz Salgado – Director de Tecnología de la Información.

## II. INFORMACIÓN GENERAL

### 2.1. OBJETIVO DE LA AUDITORÍA

Evaluar el grado de cumplimiento, eficacia y madurez del Modelo de Seguridad y Privacidad de la Información (MSPI) implementado por la Secretaría Distrital de Gobierno, verificando los componentes técnicos, organizacionales y normativos, así como la trazabilidad documental y evidencia que respalda la gestión institucional en materia de seguridad y privacidad de la información.

### 2.2. ALCANCE DE LA AUDITORÍA

La auditoría comprenderá la revisión documental y verificación de evidencias relacionadas con los componentes del MSPI, incluyendo: Gestión de la información institucional y su clasificación. Planeación de la seguridad digital. Gestión de activos de información. Gestión de riesgos de seguridad y privacidad. Control de incidentes y continuidad del servicio. Procesos de mejora y revisión por la dirección.

El período objeto de revisión será de enero a agosto de la vigencia 2025. Se verificará la conformidad con el Plan de Seguridad y Privacidad de la Información, los protocolos institucionales del Sistema Integrado de Gestión (SIG) y los lineamientos del MINTIC.

### 2.3. CRITERIOS DE LA AUDITORÍA

- Decreto 1078 de 2015 – Decreto Único Reglamentario del Sector TIC.
- Decreto 1008 de 2018 – Lineamientos generales de la Política de Gobierno Digital.
- Resolución 500 de 2021 (MINTIC) – Lineamientos y estándares de la Estrategia de Seguridad Digital; adopta el MSPI como habilitador de la Política de Gobierno Digital.
- Norma ISO/IEC 27001:2013 – Estándar internacional de gestión de seguridad de la información.
- Manual para la Implementación de la Política de Gobierno Digital, versión 7 (abril 2019).
- CONPES 3854 de 2016 – Política Nacional de Seguridad Digital.
- Documento Maestro del Modelo de Seguridad y Privacidad de la Información, MINTIC, versión 5 (21/04/2025).
- Procesos, procedimientos, manuales y planes del Sistema Integrado de Gestión (SIG) de la Secretaría Distrital de Gobierno.

- Otras normas, guías o lineamientos técnicos que resulten aplicables durante el desarrollo del proceso auditor.

## 2.4. EQUIPO AUDITOR

Peter William Vargas Pinilla / Auditor Líder
José de Jesús Gutiérrez Villalba / Auditor de Apoyo

## 2.5. METODOLOGÍA

### 1. Recolección de información

Se emitió aviso de comunicación de apertura de auditoría (donde se dio a conocer el objetivo y alcance) mediante memorando con número de radicado 20251500395963 del 20 de octubre de 2025, dirigido a la Dirección de Tecnología de la Información, en el cual se indicó que la reunión de apertura se efectuaría de manera virtual a través de la plataforma TEAMS.

De igual manera, se solicitó la participación del líder del proceso y el equipo de trabajo que considerara pertinente, así como la designación de funcionario(s) que se desempeñe(n) como enlace para atender los requerimientos propios que surjan durante el ejercicio auditor.

Así mismo, se solicitó brindar todas las facilidades al equipo auditor para el desarrollo oportuno de la actividad, incluyendo el acceso a la documentación y entrevistas que se estimen necesarias.

Se efectúo reunión de cierre el día 15 de diciembre de 2025, indicando al líder de la temática evaluada los hallazgos detectados durante el ejercicio auditor.

### 2. Apertura de Auditoría

El 23 de octubre de 2025 a las 10:00 a.m., se llevó a cabo la reunión de apertura de auditoría, con la participación del líder y el equipo de trabajo del proceso a auditar.

### 3. Entrevistas, análisis, verificación de la información y elaboración de informe.

Una vez la Dirección de Tecnologías de la Información remitió la documentación requerida, a través de las carpetas compartidas en OneDrive habilitadas por la Oficina de Control Interno, se procedió a su análisis detallado y a la verificación del cumplimiento de los lineamientos del MSPI.

Las verificaciones se realizaron mediante revisión documental, contrastación técnica y validaciones en sitio, con el acompañamiento del personal designado por la Dirección, lo que permitió corroborar la información suministrada, confirmar su trazabilidad y evaluar la aplicación práctica de los controles implementados.

La metodología empleada incluyó entrevistas dirigidas, revisión de soportes operativos, validación de matrices e instrumentos institucionales, así como observación directa de los procedimientos en ejecución. Esta combinación de técnicas permitió obtener una visión integral del funcionamiento del componente evaluado y asegurar que los resultados reflejaran el estado real de la gestión institucional frente al Modelo de Seguridad y Privacidad de la Información.

Finalizado el análisis documental, el muestreo de evidencias y las entrevistas, se registraron los hallazgos, observaciones y conclusiones. Posteriormente, se procedió con la elaboración del informe de auditoría.

## 2.6. PERÍODO DE EJECUCIÓN

Entre el 1° de enero de 2025 al 31 de agosto de 2025.

## III. DESARROLLO DE LA AUDITORIA

En el marco del modelo de operación por procesos de la Secretaría Distrital de Gobierno, se identificó que el Modelo de Seguridad y Privacidad de la Información MSPI es liderado por la Dirección de Tecnología e Información.

Realizada la revisión de los aspectos señalados en el numeral 2.5 (Metodología), la Oficina de Control Interno presenta a continuación, un análisis detallado del grado de cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI), conforme a los lineamientos establecidos en:

1. Norma ISO 27001:2013: "*Sistemas de Gestión de la Seguridad de la Información (SGSI)*".
2. Resolución 500 de 2021 (MINTIC) – Lineamientos y estándares de la Estrategia de Seguridad Digital; adopta el MSPI como habilitador de la Política de Gobierno Digital.
3. Documento Maestro del Modelo de Seguridad y Privacidad de la Información, MINTIC, versión 5 (21/04/2025).

Para la evaluación del cumplimiento, se tomaron como referencia los seis (6) pilares que estructuran la gobernanza y la operación de la seguridad digital en el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio TIC. Estos dominios constituyen el marco sobre el cual las entidades públicas implementan y fortalecen sus prácticas de seguridad y privacidad.

Desde el análisis adelantado por la Oficina de Control Interno, se validó cada uno de estos componentes como eje para verificar el nivel de madurez institucional y la efectividad de los controles asociados, lo que permitió valorar de manera integral la implementación del Modelo. Dicha evaluación se realizó a través de la aplicación de una escala porcentual compuesta por tres (3) criterios:

| Criterio | Descripción | Calificación |
|---|---|---|
| Cumple | Se ha logrado el cumplimiento de la totalidad de los requisitos evaluados | 100% |
| Parcialmente | Se evidencia un avance, pero no se cumple con la totalidad de requisitos | 50% |
| No Cumple | No se ha cumplido con ninguno de los requisitos | 0% |

Tabla N° 1 Criterios de calificación por requisito

A partir de esta calificación, se identifican **oportunidades de mejora** para los requisitos evaluados como *"No Cumple"* y *"Parcialmente"*, teniendo en cuenta las deficiencias evidenciadas y su impacto en la coherencia, gobernanza y operación del Modelo de Seguridad y Privacidad de la Información.

Estas oportunidades permiten orientar acciones correctivas y de fortalecimiento institucional, con el propósito de avanzar hacia un cumplimiento integral, trazable y sostenible del MSPI.

Para los requisitos calificados como *"Cumple"*, se recomienda mantener las prácticas y controles implementados, promoviendo su mejora continua con el fin de asegurar la sostenibilidad y el fortalecimiento del MSPI en el tiempo.

Finalmente, con base en la evidencia objetiva proporcionada por el líder del Modelo de Seguridad y Privacidad de la Información obtenida durante las verificaciones documentales y en campo, se presentan a continuación los resultados de la evaluación para cada uno de los lineamientos revisados.

## 1. Gestión de la información institucional y su clasificación

Ítems Evaluados: 11
Porcentaje de Cumplimiento: 68.2%
Madurez: En Desarrollo

| N° | Pregunta de Verificación | Nivel de Cumplimiento | Cumplimiento | Observaciones / Hallazgos |
|---|---|---|---|---|
| 1 | ¿La entidad cuenta con una política formal para la gestión, clasificación y tratamiento de la información institucional y es aprobada por el Comité de la Instancia competente? | **Cumple** | **100%** | Con relación a la verificación sobre la existencia de una política formal para la gestión, clasificación y tratamiento de la información institucional, se confirma que la entidad cuenta con un Manual de Seguridad de la Información vigente, el cual incorpora en su numeral 7 la Política de Seguridad y Privacidad de la Información.<br><br>Dicha política establece los lineamientos, criterios y controles necesarios para garantizar la adecuada administración del ciclo de vida de la información institucional, cubriendo aspectos como la clasificación, manejo, protección, acceso, conservación y disposición final de la misma.<br><br>La información contenida en el manual constituye el marco normativo interno aplicable y da cumplimiento al requisito evaluado, evidenciando que la entidad posee lineamientos formales y documentados para la gestión segura de su información. |

| N° | Pregunta de Verificación | Nivel de Cumplimiento | Cumplimiento | Observaciones / Hallazgos |
|---|---|---|---|---|
| **2** | ¿Se ha elaborado, implementado y mantenido un inventario de información institucional, incluyendo datos personales y sensibles, con criterios CID? | **Parcialmente** | **50%** | La entidad dispone de un Inventario de Información Institucional estructurado mediante el Formato GDITICFO32 V2 – Clasificación, Valoración y Clasificación de Activos de Información, el cual documenta la identificación de activos que manejan información institucional, incluyendo datos personales y sensibles.<br><br>El formato incorpora criterios de Confidencialidad, Integridad y Disponibilidad (CID) para la valoración del riesgo asociado a cada activo, lo que demuestra avances en la aplicación de lineamientos del Modelo de Seguridad y Privacidad de la Información.<br><br>No obstante, el inventario presenta brechas en su implementación y mantenimiento, particularmente en la actualización integral de los activos, la verificación de custodios y responsables, y la cobertura total de procesos que manejan datos sensibles. Por lo anterior, se evidencia un cumplimiento parcial del requerimiento evaluado.<br><br>Por lo tanto, se hace necesario actualizar y consolidar el Inventario de Información Institucional asegurando:<br>Revisión y depuración integral de los activos, incorporando todos los procesos que manejan datos personales y sensibles.<br>Identificación y formalización de custodios y responsables para cada activo, dejando la trazabilidad documentada.<br>Implementación de un procedimiento de mantenimiento periódico, que establezca frecuencia, responsables y criterios de actualización del inventario.<br>Estas acciones permitirán fortalecer la calidad del inventario, garantizar su alineación con los lineamientos del Modelo de Seguridad y Privacidad de la Información y cerrar las brechas que dieron lugar al cumplimiento parcial. |
| **3** | ¿La información se clasifica por confidencialidad, integridad y disponibilidad con metodología aprobada? | **Cumple** | **100%** | Con base en la evidencia revisada, se determinó que la entidad cumple con la aplicación de una metodología formal para la clasificación de la información bajo criterios de Confidencialidad, Integridad y Disponibilidad (CID), soportada en el Formato GDITICFO32 V2 – Clasificación, Valoración y Clasificación de Activos de Información. La herramienta se encuentra implementada y en uso para la valoración de activos, demostrando que la entidad aplica los lineamientos establecidos en el Modelo de Seguridad y Privacidad de la Información.<br><br>No obstante, se identificaron oportunidades de mejora relacionadas con la formalización del grupo encargado de la gestión de seguridad de la información y la definición de controles documentales, particularmente en lo referente al marco regulatorio interno y la ausencia de acuerdos de confidencialidad para el personal con acceso a información clasificada. Estas situaciones no afectan el cumplimiento del requerimiento, pero sí representan riesgos administrativos y operativos que requieren gestión.<br><br>Se recomienda a la entidad formalizar la estructura, roles y responsabilidades del equipo que administra la seguridad de la información, incorporando su función dentro del modelo organizacional vigente.<br><br>De igual forma, se sugiere establecer procedimientos y controles de acceso al inventario de información, incluyendo la suscripción de acuerdos de confidencialidad y la definición de criterios para la asignación, mantenimiento y revocación de permisos, con el fin de fortalecer la trazabilidad, la gobernanza y la protección de la información institucional. |
| **4** | ¿Existe un procedimiento para el etiquetado, manejo, transporte y disposición final de la información? | **Cumple** | **100%** | La entidad cuenta con una metodología formal para la clasificación de la información basada en los criterios de Confidencialidad, Integridad y Disponibilidad (CID), la cual se encuentra definida en el Procedimiento GDITIC-P004 v3 "Clasificación y Etiquetado de la Información".<br>Este procedimiento establece las directrices para categorizar la información según su nivel de sensibilidad, así como los criterios para su protección, manipulación y divulgación, garantizando la aplicación uniforme de los parámetros CID en toda la organización.<br><br>Adicionalmente, se verificó que la entidad dispone del Procedimiento GDITIC-IN021 v1 "Transporte de Información", el cual regula el tratamiento seguro de la información durante su traslado físico o digital, complementando el esquema de protección definido en la metodología de clasificación. |

| N° | Pregunta de Verificación | Nivel de Cumplimiento | Cumplimiento | Observaciones / Hallazgos |
|---|---|---|---|---|
| **5** | ¿Se aplican controles para el tratamiento de datos personales conforme a la Ley 1581 de 2012 (consentimiento, ARCO, confidencialidad)? | **No Cumple** | **0%** | La entidad dispone de la Política de Tratamiento y Protección de Datos Personales GDITIC-8002, así como de los formatos asociados GDITIC-F026, GDITIC-F027 y GDITIC-F029, los cuales establecen lineamientos generales para la recolección, uso y administración de datos personales. Estos documentos definen aspectos relacionados con el consentimiento, los derechos ARCO y los deberes de confidencialidad.<br><br>Sin embargo, durante la verificación no se evidenció la implementación efectiva de los controles requeridos por la Ley 1581 de 2012. En particular, no se encontró trazabilidad suficiente que demuestre la aplicación sistemática de:<br>Mecanismos de obtención y conservación del consentimiento informado,<br>Procedimientos operativos para el ejercicio de los derechos ARCO por parte de los titulares,<br>Controles documentados de confidencialidad aplicados al personal que trata datos personales,<br>Evidencia de seguimiento, monitoreo o verificación del cumplimiento de la política.<br><br>La ausencia de estos controles operativos demuestra que, aunque existe un marco documental, no se está aplicando de manera efectiva, por lo que el requerimiento evaluado se clasifica como no cumple. |
| **6** | ¿Se encuentran definidos los dueños y custodios de la información por proceso? | **Cumple** | **100%** | Se verificó que la entidad tiene definidos los dueños y custodios de la información por proceso, información que se encuentra documentada en la matriz GDITICFO32 V2 – Clasificación, Valoración y Clasificación de Activos de Información. Este instrumento permite identificar para cada activo su responsable funcional (dueño) y su responsable operativo (custodio), asegurando la trazabilidad sobre quién administra, autoriza, protege y mantiene la información en cada etapa de su ciclo de vida.<br><br>La existencia y uso de esta matriz evidencian la asignación formal de roles y responsabilidades, cumpliendo con el requerimiento evaluado.<br><br>No obstante, se mantienen recomendaciones previamente señaladas orientadas al fortalecimiento del proceso, sin que estas afecten el cumplimiento de la actividad auditada. |
| **7** | ¿Se evidencian mecanismos para garantizar integridad y trazabilidad de la información crítica? | **Cumple** | **100%** | Durante la verificación se constató que la entidad cuenta con mecanismos que garantizan la integridad y trazabilidad de la información crítica, los cuales se encuentran documentados y evidenciados a través de la matriz GDITICFO32 V2 – Clasificación, Valoración y Clasificación de Activos de Información.<br><br>La matriz permite identificar los activos de información críticos, sus responsables, controles asociados y criterios de valoración, lo que asegura:<br><br>Integridad: mediante la asignación de propietarios y custodios, definición de niveles de criticidad y controles aplicados a cada activo.<br><br>Trazabilidad: a través del registro documental de la ruta de administración del activo, sus responsables y las medidas de protección implementadas. |
| **8** | ¿Existen respaldos y procedimientos de restauración probados para la información crítica? | **Cumple** | **100%** | En cumplimiento de los lineamientos establecidos en la norma ISO/IEC 27001, las directrices del MINTIC para la gestión de la Seguridad y Privacidad de la Información y las actividades previstas en el plan de auditoría, existen respaldos de la información crítica y que los procedimientos de restauración han sido implementados y probados conforme a los controles definidos.<br><br>Se adjuntan las capturas y registros correspondientes como evidencia objetiva de las validaciones realizadas. Esta información se entrega atendiendo a su carácter sensible y garantizando la trazabilidad del proceso, bajo los principios de confidencialidad, integridad y disponibilidad. La evidencia compartida permite verificar la ejecución y efectividad de los mecanismos de copia de seguridad y recuperación, así como el cumplimiento de los requisitos de continuidad y protección de la información establecidos por la organización |
| **9** | ¿Se controla el acceso a la información de acuerdo con la clasificación y necesidad de conocer? | **No Cumple** | **0%** | La entidad reporta como soporte el Directorio Activo de la Información, el cual permite administrar usuarios, roles y permisos de acceso. Sin embargo, durante la verificación no se evidenció que dichos permisos estén articulados con la clasificación de la información ni con el principio de necesidad de conocer, tal como exige el Modelo de Seguridad y Privacidad de la Información.<br><br>Adicionalmente, se encuentra pendiente la verificación de los Acuerdos de Nivel de Servicio (ANS) asociados a la gestión de accesos, lo cual impide confirmar la existencia de controles formales, documentados y verificables que regulen el acceso en función del nivel de sensibilidad del activo y del rol del funcionario. |

| N° | Pregunta de Verificación | Nivel de Cumplimiento | Cumplimiento | Observaciones / Hallazgos |
|---|---|---|---|---|
| **10** | ¿Se realiza capacitación periódica al personal sobre gestión y clasificación de la información? | **Parcialmente** | **50%** | Con relación a la verificación del cumplimiento del requisito asociado a la capacitación periódica en gestión y clasificación de la información, se identificó evidencia del desarrollo de dos (2) sesiones formativas relacionadas con el tema de Activos de Información: la primera realizada el 10 de febrero para personal del nivel central y la segunda el 7 de abril dirigida a funcionarios de las localidades.<br><br>Si bien estas actividades evidencian esfuerzos institucionales en materia de sensibilización y formación, no se observa una programación formal ni un ciclo periódico de capacitación que permita demostrar cumplimiento pleno del criterio establecido. En consecuencia, y con base en la trazabilidad documental revisada, se determina que el requisito se cumple parcialmente. |
| **11** | ¿Se actualiza el inventario de información mediante proceso de mejora continua y se reporta al Comité de la Instancia competente? | **Parcialmente** | **50%** | Se verificó que la entidad realiza actualizaciones periódicas del Inventario de Información Institucional, integrándolo al proceso de mejora continua, lo cual evidencia que existe gestión activa para mantener vigente la identificación, clasificación y valoración de los activos de información.<br><br>Sin embargo, se constató que estas actualizaciones no han sido reportadas al Comité de la Instancia competente, instancia encargada de revisar, validar y hacer seguimiento a los elementos estratégicos del Modelo de Seguridad y Privacidad de la Información. |

Tabla N° 2 Gestión de la información institucional y su clasificación

Los resultados consolidados fueron los siguientes:

- **6 ítems con Cumplimiento (100%)**
- **3 ítems con Cumplimiento Parcial (50%)**
- **2 ítems con No Cumplimiento (0%)**

Dicho comportamiento evidencia avances importantes en materia de lineamientos normativos, documentación, mecanismos técnicos y asignación de roles; sin embargo, también pone de manifiesto brechas relacionadas con la actualización, trazabilidad y aplicación operativa de los controles previstos en el Modelo de Seguridad y Privacidad de la Información (MSPI).

**1. Temáticas con Cumplimiento Parcial (50%)**

A continuación, se consolidan las temáticas que alcanzaron un nivel de cumplimiento del **50%**, junto con el análisis de las causas principales y las oportunidades de mejora identificadas.

- **Temática N° 2. Inventario de información institucional**

Aunque la entidad dispone de un inventario estructurado que incorpora criterios CID y se encuentra soportado en el Formato **GDITIC-FO32 V2**, la verificación permitió identificar brechas en:

- La cobertura total de los procesos que administran datos personales y sensibles.
- La actualización integral y depuración de activos.
- La formalización de custodios y responsables.
- La definición de un ciclo periódico de actualización.

**Impacto:** limita la trazabilidad del activo y el control sobre su ciclo de vida. **Oportunidad de mejora:** establecer una rutina anual o semestral de actualización, que incluya responsables, frecuencia y mecanismos de verificación.

- **Temática N° 10. Capacitación periódica**

Se evidencia la realización de dos sesiones formativas; sin embargo:

- No existe un plan anual de formación asociado al MSPI.
- No se cuenta con un programa sistemático ni con un mecanismo de registro y seguimiento.
- No se demuestra cobertura institucional suficiente.

**Impacto:** dificulta la apropiación del modelo y la aplicación homogénea de los controles. **Oportunidad de mejora:** incorporar estas capacitaciones al **Plan Institucional de Capacitación (PIC)** y definir un ciclo mínimo (semestral o anual).

- **Temática N° 11. Actualización del inventario y reporte al Comité**

Si bien se evidencian ajustes periódicos al inventario, no se encontró evidencia de:

- Reportes formales al Comité de la Instancia competente.
- Seguimiento o validación por parte del nivel directivo, como exige el MSPI.

**Impacto:** debilita la gobernanza del modelo y la validación institucional del componente de información. **Oportunidad de mejora:** incorporar el informe de actualización del inventario como tema permanente en la agenda del comité.

**2. Temáticas No Cumplidas (0%)**

Las siguientes temáticas obtuvieron calificación del **0%**, evidenciando ausencia total de implementación operativa pese a la existencia de lineamientos documentales. Estas brechas representan riesgos significativos para la institución, tanto en materia legal como de seguridad de la información.

- **Temática N° 5. Implementación de la Ley 1581 de 2012**

Si bien la entidad cuenta con una Política de Tratamiento de Datos Personales y formatos asociados, no se evidenció la existencia de mecanismos operativos que permitan demostrar su implementación. Durante la verificación se identificaron las siguientes situaciones:

- No se encontró **trazabilidad del consentimiento informado**, ni repositorios que evidencien su obtención y conservación.
- No se evidenció la aplicación de **procedimientos ARCO** (Acceso, Rectificación, Cancelación y Oposición).
- No existen **controles documentados de confidencialidad** aplicables al personal con acceso a datos personales o sensibles.
- No se encontraron **actividades de monitoreo o seguimiento** que evalúen el cumplimiento de la política o el estado del sistema de protección de datos.

**Riesgo asociado:**

Estas debilidades pueden conllevar a **incumplimiento legal directo**, posibles sanciones administrativas ante la SIC y exposición a eventos reputacionales que afecten la confianza institucional, al no garantizar la protección adecuada de la información personal que administra la entidad.

- **Temática N° 9. Control de accesos según clasificación y necesidad de conocer**

La entidad dispone del Directorio Activo como herramienta tecnológica para la administración de usuarios, roles y permisos; sin embargo, no se evidenció articulación entre la gestión de accesos y los lineamientos del MSPI. Específicamente:

- Los accesos **no están vinculados al nivel de clasificación** de la información (CID).
- No se aplican controles alineados al **principio de necesidad de conocer**, lo cual es requisito fundamental del modelo.
- No existen **Acuerdos de Nivel de Servicio (ANS)** o mecanismos verificables que regulen la asignación, revisión, modificación y revocación de accesos.
- No se evidencia un proceso formal de **auditoría de permisos** o de validación periódica por parte de los dueños de información.

**Riesgo asociado:** Esto puede derivar en **sobreexposición de información crítica o sensible**, accesos no autorizados y ausencia de segregación de funciones, lo que afecta la integridad, confidencialidad y trazabilidad de los activos institucionales.

Con base en los resultados obtenidos, el componente Gestión de la Información Institucional y su Clasificación alcanzó un nivel de avance del 68%, lo que confirma que la entidad cuenta con un marco documental adecuado, alineado a los lineamientos del MSPI y a normas de referencia como ISO/IEC 27001.

No obstante, las principales brechas se ubican en la implementación operativa de los controles, más que en su diseño. Esto evidencia que:

- Las políticas y procedimientos existen.
- Pero no se aplican de forma consistente, sistemática ni verificable en la operación.
- Los controles clave para la protección de la información presentan deficiencias en trazabilidad, sostenibilidad y monitoreo.

Esta situación limita la madurez del modelo y afecta la capacidad de garantizar un manejo seguro y responsable de la información institucional.

## 2. Planeación de a Seguridad Digital

Ítems Evaluados: 12

Porcentaje de Cumplimiento: 91.7%

Madurez: Consolidado

| Nº | Pregunta de Verificación | Nivel de Cumplimiento | Cumplimiento | Observaciones / Hallazgos |
|---|---|---|---|---|
| 1 | ¿La entidad cuenta con un Plan de Seguridad y Privacidad de la Información vigente, aprobado y divulgado? | **Cumple** | **100%** | Durante la revisión documental se verificó la existencia del Plan de Seguridad y Privacidad de la Información GDI-TIC PL002, el cual se encuentra vigente, formalmente aprobado y disponible para consulta por parte de los funcionarios. La documentación revisada cumple con los requisitos establecidos en el Modelo de Seguridad y Privacidad de la Información y se encuentra alineada con las directrices del MINTIC para la gestión de la seguridad de la información.<br><br>La evidencia aportada permite confirmar la disponibilidad, validez y divulgación del instrumento, por lo que, con base en la verificación efectuada y la trazabilidad documental se concluye que el requisito se cumple. |
| 2 | ¿El Plan SPI establece metas, indicadores y metodología de medición consistentes con FURAG / MSPI? | **Cumple** | **100%** | Se verificó que el Plan de Seguridad y Privacidad de la Información (Plan SPI) establece metas, indicadores y una metodología de medición alineadas con los lineamientos del FURAG y del Modelo de Seguridad y Privacidad de la Información (MSPI). El documento integra parámetros de seguimiento, periodicidad, responsables y criterios de evaluación que permiten medir el avance del modelo conforme a los estándares institucionales.<br><br>Durante la revisión se evidenciaron los niveles de avance reportados (74,5% en nivel local y 98,33% en nivel central). Si bien estos porcentajes reflejan oportunidades de mejora en la ejecución, no afectan la consistencia técnica del Plan SPI, ni su alineación con las exigencias metodológicas del FURAG/MSPI.<br><br>Por lo anterior, se concluye que el requerimiento evaluado se cumple, dado que el Plan SPI sí define metas, indicadores y metodología de medición consistentes con los marcos establecidos. |
| 3 | ¿El Plan SPI se articula con el PETI/SIG/plan institucional y con el presupuesto? | **Cumple** | **100%** | En el marco de la verificación del criterio asociado a la articulación del Plan de Seguridad y Privacidad de la Información (SPI) con los instrumentos de planeación institucional, se revisó el Plan Estratégico de Tecnologías de la Información – PETI (GDI-TIC-PL001). La documentación evidencia la alineación entre los objetivos, líneas estratégicas y acciones del PETI y los componentes del Plan SPI, demostrando coherencia con el Sistema Integrado de Gestión (SIG) y los instrumentos de planeación institucional vigentes.<br><br>Adicionalmente, se constató que la programación definida en el PETI incorpora requerimientos asociados a seguridad y privacidad de la información, integrándose a la asignación presupuestal prevista para la gestión TIC. |
| 4 | ¿Se encuentran definidos roles, responsabilidades y comités para la seguridad digital? | **Cumple** | **100%** | En el marco de la verificación del criterio relacionado con la definición de roles, responsabilidades y comités para la seguridad digital, se revisó el Manual de Gestión de Seguridad de la Información GDITICM004, así como el Procedimiento de Identificación y Valoración de Activos de Información GDITICP004. La documentación consultada establece de manera formal la estructura de gobernanza del Modelo de Seguridad y Privacidad de la Información, incluyendo los roles responsables, sus funciones, niveles de autoridad y los mecanismos de coordinación institucional. |
| 5 | ¿Se gestiona el cambio organizacional y tecnológico relacionado con el Plan SPI? | **Cumple** | **100%** | Se verificó que la entidad gestiona los cambios organizacionales y tecnológicos asociados al Plan de Seguridad y Privacidad de la Información (Plan SPI) mediante la aplicación del Procedimiento GDITIC-P011 – Implementación de Cambios, referido en el numeral 7.1.2 – Gestión de Cambios.<br><br>La existencia y aplicación de este procedimiento demuestran que la entidad cuenta con un mecanismo formal y operativo para gestionar los cambios que puedan afectar el Modelo de Seguridad y Privacidad de la Información, cumpliendo con el requerimiento evaluado. |
| 6 | ¿Se realiza seguimiento trimestral al Plan SPI y se reporta a la alta dirección? | **Parcialmente** | **50%** | Se revisó la documentación relacionada con el seguimiento trimestral al Plan de Seguridad y Privacidad de la Información (Plan SPI) y se verificó la existencia de informes de avance correspondientes al I, II y III trimestre de 2025, preparados por el "Grupo" de Seguridad de la Información. Entre la evidencia analizada se encontraron:<br><br>Copia del Informe de Avance del Plan SPI – Trimestre 2 de 2025,<br>Capturas de pantalla de los repositorios institucionales con carpetas denominadas I Trimestre, II Trimestre y III Trimestre,<br>Documentos cargados que incluyen informes de avance del Plan de Gestión, Plan de Tratamiento de Riesgos, Gestión TIC e informes PSPI para los trimestres 1, 2 y 3 de 2025, |

| N° | Pregunta de Verificación | Nivel de Cumplimiento | Cumplimiento | Observaciones / Hallazgos |
|---|---|---|---|---|
| | | | | Matriz del Plan de Gestión – Gerencia TIC y el Plan SPI vigente.<br><br>La evidencia confirma que sí se realiza seguimiento trimestral al Plan SPI y que la entidad mantiene registro documental organizado del proceso. Sin embargo, se observó que los informes no cuentan con firmas de elaboración y aprobación, y no se evidenció trazabilidad que demuestre el reporte formal de dichos informes a la alta dirección, elemento requerido por la actividad evaluada. |
| **7** | ¿La entidad dispone de recursos técnicos y humanos suficientes para ejecutar el Plan SPI? | **Cumple** | **100%** | Se verificó que la entidad dispone de recursos técnicos y humanos suficientes para la ejecución del Plan de Seguridad y Privacidad de la Información (Plan SPI). Como soporte se revisó el Proyecto 8048 – Vigencia 2025, en el cual se encuentra prevista la contratación de personal especializado, incluyendo ingenieros de apoyo y el Oficial de Seguridad de la Información, figura clave para la administración, coordinación y seguimiento del modelo SPI.<br><br>La asignación de estos recursos garantiza la capacidad operativa necesaria para implementar las acciones del Plan SPI, ejecutar sus actividades técnicas, mantener los controles definidos y asegurar la continuidad del modelo. |
| **8** | ¿Se encuentra adoptada la Política de Seguridad Digital como habilitador de Gobierno Digital? | **Cumple** | **100%** | Se verificó que la entidad ha adoptado formalmente la Política de Seguridad Digital como parte de los habilitadores del Modelo de Gobierno Digital, en concordancia con los lineamientos del Ministerio TIC y el marco normativo vigente.<br><br>La política se encuentra definida, documentada y articulada con los instrumentos institucionales de gestión de riesgos, seguridad de la información y continuidad operativa, constituyéndose en el marco directivo que orienta la protección de los activos tecnológicos, la gestión de incidentes y el aseguramiento de los servicios digitales. |
| **9** | ¿Se integra la medición de seguridad digital con los instrumentos del MIPG y FURAG? | **Cumple** | **100%** | Se verificó que la entidad integra la medición de seguridad digital con los instrumentos del MIPG y el FURAG, conforme a los lineamientos establecidos por el Ministerio TIC. Como soporte se revisó el Instrumento emitido por MINTIC el 18 de junio de 2025, el cual establece los criterios y parámetros para la medición unificada de seguridad digital dentro del marco del Modelo Integrado de Planeación y Gestión (MIPG). |
| **10** | ¿Se gestionan riesgos de terceros y proveedores de TI (contratos con cláusulas de seguridad y privacidad)? | **Parcialmente** | **50%** | Se verificó la gestión de riesgos asociados a terceros y proveedores de TI mediante la revisión de estudios previos, matrices de riesgos institucionales y los registros de riesgos de seguridad y privacidad de la información. La información reportada evidencia un avance parcial en la incorporación y seguimiento de riesgos relacionados con terceros, así como en la definición de controles contractuales (cláusulas de seguridad y privacidad).<br><br>A nivel central, se identifica un avance del 65,20%, con plazo de cierre establecido al 30 de septiembre. En el caso de las localidades, el avance reportado corresponde al 33%, con fecha de cumplimiento programada para noviembre. No obstante, se observa que la cobertura de riesgos vinculados a proveedores de TI y la formalización de cláusulas contractuales aún no es completa ni homogénea entre las dependencias evaluadas.<br><br>En consecuencia, la evidencia demuestra que el proceso de gestión de riesgos de terceros se encuentra implementado de manera parcial, requiriendo ajustes para garantizar una trazabilidad completa, la estandarización de controles y la incorporación integral de criterios de seguridad y privacidad en los contratos y acuerdos de servicio. |
| **11** | ¿El Plan SPI detalla las actividades de trabajo, con responsables, alcance, vigencia y plazos definidos para su ejecución? | **Cumple** | **100%** | Se revisó el Plan de Seguridad y Privacidad de la Información – Plan SPI (Código: GDI-TIC-PL002, Versión 7, con vigencia a partir del 28 de enero de 2025), verificándose que el documento establece de forma explícita las actividades de trabajo, sus responsables, el alcance, la vigencia y los plazos definidos para su ejecución.<br><br>La evidencia se respalda con la captura de la sección 2.4 – Detalles de actividades del plan de trabajo, en la cual se presenta información estructurada que permite asegurar la trazabilidad del proceso.<br><br>La documentación revisada demuestra que el Plan SPI define de manera completa y consistente las actividades, responsables, alcance, vigencias y tiempos de ejecución, cumpliendo con los requisitos de planificación exigidos en materia de seguridad y privacidad de la información |
| **12** | ¿El Plan SPI incluye un mecanismo de seguimiento, evaluación y actualización de metas e indicadores, conforme a la metodología aprobada por el Comité de la Instancia competente? | **Cumple** | **100%** | Se verificó que el Plan de Seguridad y Privacidad de la Información (Plan SPI) incorpora un mecanismo formal de seguimiento, evaluación y actualización de metas e indicadores.<br><br>El análisis documental evidencia que el Plan SPI establece:<br>Lineamientos de seguimiento periódico para la medición del avance de metas e indicadores.<br>Criterios de evaluación que permiten verificar desempeño, cumplimiento y desviaciones frente a los parámetros definidos. |

| N° | Pregunta de Verificación | Nivel de Cumplimiento | Cumplimiento | Observaciones / Hallazgos |
|---|---|---|---|---|
| | | | | Procedimiento de actualización, en el cual se contemplan ajustes al plan y a sus indicadores con base en los resultados de monitoreo, retroalimentación institucional y validación según la metodología aprobada por el Comité de la Instancia competente. |

Tabla N° 3 Planeación de a Seguridad Digital

Los resultados evidencian que, para el componente de Planeación de la Seguridad Digital, de las doce (12) temáticas analizadas, diez (10) alcanzan un cumplimiento del 100% y únicamente dos (2) registran un cumplimiento del 50%. Estas situaciones puntuales representan aspectos susceptibles de fortalecimiento, cuya atención permitirá consolidar la planeación en materia de seguridad digital y mantener la uniformidad en la implementación del MSPI.

El nivel de cumplimiento evidencia un estado de madurez consolidado, con una estructura de planeación sólida y alineada a los lineamientos normativos (MSPI, FURAG, MIPG, MINTIC).

Los patrones observados consolidan que la entidad cuenta con:

- ✓ Instrumentos institucionales vigentes, aprobados y divulgados, con trazabilidad verificable.
- ✓ Articulación estratégica clara, integrando el Plan SPI con PETI, SIG, presupuesto e instrumentos de medición nacional.
- ✓ Gobernanza y responsabilidades definidas, soportadas en manuales y procedimientos aprobados.
- ✓ Metodología de seguimiento y actualización formalizada, con criterios de medición que aseguran consistencia técnica.

En general, los elementos revisados demuestran consistencia documental, alineación institucional y capacidad operativa para administrar la seguridad y privacidad de la información.

Con fundamento en lo anteriormente expuesto, la Oficina de Control Interno formula la Fortaleza N° 1 Consolidación de la Gobernanza y la Gestión de Riesgos del componente "Planeación de la Seguridad Digital en el componente "*Planeación de la Seguridad Digital*"

**1. Temáticas con cumplimiento parcial (50%)**

Las siguientes temáticas registraron cumplimiento parcial, constituyéndose en oportunidades de mejora:

- **Temática N° 6. Seguimiento Trimestral al Plan SPI**

La entidad sí realiza el seguimiento trimestral al Plan de Seguridad y Privacidad de la Información y mantiene registro documental organizado, lo cual confirma la existencia del proceso operativo de monitoreo. Sin embargo, la verificación detallada del expediente demostró brechas en formalización y gobernanza, particularmente en:

- ✓ Ausencia de firmas de elaboración, revisión y aprobación en los informes trimestrales consultados.
- ✓ No existencia de trazabilidad formal del reporte a la Alta Dirección o al Comité competente.

- ✓ Inexistencia de evidencia documental que demuestre análisis, retroalimentación o decisiones derivadas de los informes presentados.

Esto implica que, aunque el proceso de seguimiento está en marcha y genera productos, el ciclo de control no se cierra, debido a la falta de validación formal y ausencia de evidencia del proceso de reporte y toma de decisiones.

La brecha afecta la gobernanza del modelo, la trazabilidad institucional y el cumplimiento estricto del MSPI en materia de gestión y rendición de cuentas.

- **Temática N° 10. Gestión de Riesgos de Terceros y Proveedores TI**

Existen avances en la gestión de riesgos asociados a terceros y proveedores de TI, respaldados en matrices institucionales, estudios previos y registros de riesgos del módulo de seguridad y privacidad. No obstante, persisten brechas que reflejan una implementación parcial y no homogénea entre el nivel central y las localidades, particularmente en aspectos críticos del proceso.

- ✓ Entre las principales debilidades identificadas se encuentran:
- ✓ Cobertura incompleta en la identificación, valoración y seguimiento de riesgos de terceros.
- ✓ Incorporación no homogénea de cláusulas de seguridad y privacidad en contratos y acuerdos de servicio
- ✓ Desbalance en el nivel de avance, evidenciado en: 65,2% en nivel central y 33% en localidades.

Estas brechas evidencian la necesidad de fortalecer el aseguramiento contractual, mejorar la coordinación entre dependencias y consolidar una metodología única que permita gestionar los riesgos derivados de terceros de manera integral y consistente. Dado que estos riesgos constituyen un vector crítico para la seguridad institucional, su tratamiento oportuno y estandarizado resulta fundamental para garantizar el cumplimiento normativo y la protección de los servicios y activos de información.

Con fundamento en lo anteriormente expuesto, la Oficina de Control Interno formula la Observación N° 2 Aspectos por Mejorar en el Seguimiento Institucional y la Gestión de Riesgos con Terceros del componente "*Planeación de la seguridad digital*".

### 3. Gestión de Activos de Información

Ítems Evaluados: 12
Porcentaje de Cumplimiento: 91.7%
Madurez: Consolidado

| N° | Pregunta de Verificación | Nivel de Cumplimiento | Cumplimiento | Observaciones / Hallazgos |
|---|---|---|---|---|
| 1 | ¿Existe un inventario de activos de información (hardware, software, datos, servicios) por dependencia? | Cumple | 100% | Se confirmó la existencia de un inventario institucional de activos de información que consolida los elementos de hardware, software, datos y servicios, estructurado por cada dependencia. La verificación se realizó mediante la revisión de la Matriz de Activos de Información, documento que contiene el registro detallado de los activos, su clasificación, ubicación administrativa y tecnológica, así como los responsables asignados para su gestión. |

| N° | Pregunta de Verificación | Nivel de Cumplimiento | Cumplimiento | Observaciones / Hallazgos |
|---|---|---|---|---|
| **2** | ¿Los activos están clasificados por criticidad y criterios CID? | **Cumple** | **100%** | Captura de pantalla que muestra el cargue de información referente a: Formatos gdi tic 032-V2 ALK, gdi tic 032-V2 AL Engativá, gdi tic 032-V2 Matriz activos de infor ALCB actualizada 19062025, gdi tic 032-V2 Paranda 04-06 -2025 ALPA, gdi tic 032-V2 GTH. Matriz Activos de Información Teusaquillo, Tunjuelito, Mártires, San Cristóbal, Suba, OAP, OCI, Contratación, Dirección Jurídica, DGAEP, DAE, SAC, Administrativa, despacho y diálogo social |
| **3** | ¿Cada activo tiene propietario designado y definido en el inventario? | **Cumple** | **100%** | Se verificó que el inventario institucional de activos de información incorpora de manera explícita la asignación de roles de propiedad, custodia y producción de la información para cada activo registrado. La revisión de la Matriz de Activos de Información evidencia que, para cada elemento (hardware, software, datos y servicios), se encuentran definidos:<br>Propietario del activo, responsable de su administración funcional y del aseguramiento de su disponibilidad y uso adecuado.<br>Custodio del activo, encargado de la administración operativa, preservación y soporte técnico asociado.<br>Productor de la información, cuando aplica, responsable de la creación, actualización y calidad de los datos. |
| **4** | ¿Se encuentran definidos y aplicados controles de acceso por roles y necesidad de conocer? | **Cumple** | **100%** | Se verificó que la entidad cuenta con controles de acceso definidos y aplicados bajo el principio de roles y necesidad de conocer, conforme a los lineamientos del Modelo SPI. La revisión del documento GDI-TIC-F032 – Identificación, Valoración y Clasificación de Activos de Información evidencia que el proceso de clasificación incluye parámetros explícitos para determinar los niveles de acceso requeridos según la sensibilidad del activo, el perfil del usuario y las responsabilidades asociadas. |
| **5** | ¿Se aplican controles físicos y ambientales para los activos críticos (CPD, oficinas, archivo)? | **Parcialmente** | **50%** | Se efectuó la revisión del Manual de Gestión de Seguridad de la Información – GDI-TIC-M004, específicamente el numeral 7.1.6, en el cual se establecen lineamientos para la aplicación de controles físicos y ambientales sobre activos críticos, incluyendo centros de procesamiento de datos (CPD), oficinas y áreas de archivo. El documento evidencia que existen disposiciones formales para la protección de áreas sensibles, restricciones de acceso y medidas de control ambiental.<br><br>Durante la verificación en sitio y documental se identificó que:<br>La entidad cuenta con ocho (8) cuartos técnicos a nivel central, los cuales disponen de un mecanismo de control de acceso mediante tarjeta única. No obstante, este mecanismo permite el ingreso de múltiples personas sin un registro individualizado, lo que limita la capacidad de trazabilidad y dificulta la verificación precisa de quién accedió a cada área.<br><br>El numeral 7.1.6.2 – Áreas restringidas establece la existencia de zonas de acceso controlado; sin embargo, no se encontró documentación que identifique de manera específica cuáles son estas áreas, tanto en el nivel central como en las localidades.<br><br>La ausencia de un inventario formal de áreas críticas y la falta de mecanismos que garanticen un control de acceso individualizado representan brechas en la aplicación efectiva de los controles físicos definidos en el manual.<br><br>Si bien la entidad cuenta con lineamientos y mecanismos iniciales que demuestran la existencia de controles físicos y ambientales para la protección de activos críticos, su implementación no es completa ni plenamente trazable, lo que impide asegurar un control robusto y verificable según los estándares del Modelo SPI. |
| **6** | ¿Se gestionan formalmente los cambios sobre activos críticos (configuración, parches, versiones)? | **Cumple** | **100%** | Durante la verificación del criterio relacionado con la gestión formal de cambios sobre activos críticos —incluyendo configuraciones, parches y versiones— se revisó el Manual de Gestión de Seguridad de la Información GDITICM004, específicamente el numeral 7.1.1.1, así como el Procedimiento de Identificación y Valoración de Activos de Información GDITICP004. Ambos documentos establecen lineamientos y actividades formales para el tratamiento, control y registro de cambios aplicados a los activos clasificados como críticos. |
| **7** | ¿Se realizan respaldos periódicos y pruebas de restauración en activos críticos? | **Cumple** | **100%** | Se verificó que la entidad implementa un proceso formal de respaldos (backups) periódicos para los activos críticos de información, en concordancia con los lineamientos del Modelo SPI y las buenas prácticas de continuidad del negocio. La revisión documental y técnica evidencia la existencia de procedimientos establecidos para la generación, almacenamiento y control de copias de seguridad. |

| N° | Pregunta de Verificación | Nivel de Cumplimiento | Cumplimiento | Observaciones / Hallazgos |
|---|---|---|---|---|
| **8** | ¿Se gestiona el ciclo de vida de los activos (adquisición, operación, disposición segura)? | **Cumple** | **100%** | Se revisó el Manual de Gestión de Seguridad de la Información – GDI-TIC-M004, específicamente el numeral 7.1.9.1 – Requisitos de seguridad de los sistemas de información, el cual establece lineamientos para la gestión del ciclo de vida de los activos, contemplando las fases de adquisición, operación y disposición segura. El manual define las obligaciones institucionales para asegurar que los activos sean gestionados bajo criterios de seguridad desde su incorporación hasta su retiro.<br><br>Durante la verificación se constató que la entidad cuenta con instrumentos normativos asociados al proceso, entre ellos el Procedimiento GDI-TIC-P002, que contempla la sección "Metodología de desarrollo", la cual orienta la incorporación de requisitos de seguridad en el ciclo de vida de los activos y su integración en los procesos de administración tecnológica. |
| **9** | ¿Se controla el uso de software autorizado y se previene software no licenciado? | **Cumple** | **100%** | Se revisó el Manual de Gestión de Seguridad de la Información – GDI-TIC-M004, específicamente el numeral 7.1.7.8 – Instalación de software en los sistemas operativos, el cual establece de manera explícita las directrices para el control del uso de software autorizado y la prevención de instalación o utilización de software no licenciado dentro de la entidad.<br><br>La evidencia documental permite verificar que:<br>La instalación de software se encuentra restringida a personal autorizado, bajo lineamientos definidos por el área de TI.<br>Se establece la obligación de utilizar únicamente software licenciado, validado y aprobado institucionalmente, garantizando cumplimiento legal y técnico.<br>Se contemplan controles para impedir o detectar la presencia de software no autorizado, incluyendo revisión periódica, validaciones de cumplimiento y restricciones de privilegios de instalación.<br>Se documenta el proceso de aprobación, registro y control de software implementado en los equipos corporativos, asegurando trazabilidad y evidencia de licenciamiento.<br>Los lineamientos están alineados con las prácticas del Modelo SPI y con los requisitos de protección de activos tecnológicos. |
| **10** | ¿Se evalúan y gestionan los riesgos de servicios en la nube y terceros que operan activos? | **Parcialmente** | **50%** | Se revisó la Matriz de Riesgos de Contratación (Código GCO-GCI-F164, Versión 01, Vigencia desde el 16 de diciembre de 2021, Caso HOLA: 206942), correspondiente al contrato cuyo objeto es "Prestar el Servicio Integral de Telecomunicaciones a la Secretaría Distrital de Gobierno". La matriz evidencia que se han identificado y valorado ciertos riesgos asociados a la prestación del servicio por parte del proveedor, incluyendo aspectos operativos y de continuidad.<br><br>Sin embargo, el análisis técnico permitió establecer que:<br>La matriz revisada no incorpora riesgos específicos de seguridad y privacidad de la información, pese a que el servicio contratado implica tratamiento, transmisión o gestión de datos y servicios tecnológicos que pueden impactar activos críticos.<br>La ausencia de riesgos SPI limita la capacidad institucional para evaluar amenazas propias de terceros que operan activos o prestan servicios tecnológicos, incluyendo los controles necesarios para su tratamiento.<br>La trazabilidad documental demuestra que, si bien existe gestión parcial del riesgo contractual, no se integra plenamente la perspectiva de riesgo de seguridad y privacidad exigida por el Modelo SPI. |
| **11** | ¿Se generan y revisan registros de actividad sobre activos críticos para detectar anomalías? | **Cumple** | **100%** | Se verificó que la entidad genera, documenta y revisa registros de actividad asociados a activos críticos, con el fin de identificar anomalías operativas, cambios no autorizados y eventos que puedan comprometer la integridad, disponibilidad o seguridad de los sistemas.<br><br>La revisión documental incluyó:<br>Manual de Gestión de Seguridad de la Información<br>Código GDI-TIC-M004, Versión 11, Vigencia desde 4 de diciembre de 2024.<br><br>Secciones 7.1.7 – Política de Seguridad en las Operaciones, 7.1.7.1 – Procedimientos de operación documentados y 7.1.7.2 – Gestión de Cambios, las cuales establecen lineamientos específicos para el registro, monitoreo y control de actividades operativas sobre activos críticos.<br>Procedimiento de Control de Cambios<br>Código GDI-TIC-P011, Versión 01, Vigencia desde 28 de septiembre de 2023.<br>El procedimiento define los mecanismos para documentar solicitudes de cambio, autorizaciones, validaciones técnicas, ejecuciones y verificaciones posteriores.<br>Reporte Consolidado de Procesos de Control de Cambios<br>Documento que compila los registros generados entre enero y agosto de 2025, evidenciando la trazabilidad de las actividades realizadas, los cambios aplicados, su clasificación, responsables y validaciones correspondientes. |

| N° | Pregunta de Verificación | Nivel de Cumplimiento | Cumplimiento | Observaciones / Hallazgos |
|---|---|---|---|---|
| 12 | ¿La entidad elaboró y mantiene actualizado el inventario de activos de seguridad y privacidad de la información, clasificado según criterios de confidencialidad, integridad y disponibilidad, y aprobado por el Comité de la Instancia competente? | **Cumple** | **100%** | Se verificó que la entidad elaboró y mantiene actualizado el inventario de activos de seguridad y privacidad de la información, estructurado conforme a los criterios de confidencialidad, integridad y disponibilidad (CID) definidos en el Modelo SPI. La revisión evidenció que el inventario se encuentra diligenciado por múltiples dependencias y localidades, y está soportado en el formato institucional GDI-TIC-032 (Versión 2).<br><br>Como evidencia, se revisaron capturas de pantalla que muestran el cargue de información correspondiente a los siguientes registros:<br><br>Formatos GDI-TIC-032-V2 de: ALK, AL Engativá, ALCB (actualizada al 19-06-2025), ALPA (04-06-2025), GTH.<br><br>Matrices de Activos de Información de las localidades y dependencias:<br>Teusaquillo, Tunjuelito, Los Mártires, San Cristóbal, Suba, Oficina Asesora de Planeación (OAP), Oficina de Control Interno (OCI), Contratación, Dirección Jurídica, DGAEP, DAE, SAC, Dirección Administrativa, Despacho y Diálogo Social.<br><br>La verificación documental permitió confirmar que:<br>Los activos se encuentran identificados, clasificados y registrados con sus atributos CID. La información está actualizada y corresponde a diferentes unidades operativas de nivel central y localidades.<br><br>El inventario sigue la estructura y lineamientos del Modelo SPI, asegurando trazabilidad, completitud y estandarización. |

Tabla N° 4 Gestión de Activos de Información

Los resultados evidencian que, para el componente de Gestión de Activos de Información, de las doce (12) temáticas analizadas, diez (10) alcanzan un cumplimiento del 100% y únicamente dos (2) registran un cumplimiento del 50%. Estas situaciones puntuales representan aspectos susceptibles de fortalecimiento, cuya atención permitirá consolidar la administración institucional de los activos de información y mantener la uniformidad en la implementación del MSPI.

El nivel de cumplimiento obtenido evidencia un estado de madurez significativo, respaldado en la existencia de herramientas, procesos y lineamientos que estructuran adecuadamente la gestión de activos. El análisis refleja que la entidad ha desarrollado una arquitectura operativa y documental consistente, alineada a los lineamientos normativos del **MSPI**, así como a las buenas prácticas de seguridad de la información.

En conjunto, estos elementos demuestran consistencia documental, alineación institucional y capacidad operativa para administrar los activos de información bajo los lineamientos del MSPI.
Con fundamento en lo anteriormente expuesto, la Oficina de Control Interno formula la Fortaleza N° 2 Madurez Documental y Operativa en la Gestión de Activos de Información en el componente "*Gestión de activos de información*"

**1. Temáticas con cumplimiento parcial (50%)**

Las siguientes temáticas registraron cumplimiento parcial, constituyéndose en oportunidades de mejora:

**Temática N° 5. Controles físicos y ambientales (50%)**
Se identificó que algunos cuartos técnicos permiten el ingreso de personal sin contar con registros individualizados que permitan evidenciar quién accedió y en qué momento; esta situación limita la trazabilidad del acceso y reduce la efectividad de los controles implementados para la protección de áreas críticas y activos sensibles. Adicionalmente, no se cuenta con un inventario institucional formal que identifique de manera específica las áreas críticas, lo que dificulta la delimitación y el control de zonas restringidas.

En términos de seguridad, la ausencia de control individual de accesos y de una definición clara de áreas restringidas afecta la aplicación efectiva de los controles establecidos por el Modelo SPI.

**Temática N° 10. Gestión de riesgos en la nube y terceros (50%)**
En relación con la gestión de riesgos en la nube y terceros, se evidenció que, si bien existe gestión contractual, esta no integra de manera completa los riesgos de seguridad y privacidad de la información.

La matriz revisada no contempla riesgos SPI, a pesar de tratarse de un servicio que implica tratamiento, transmisión y operación de datos y activos tecnológicos. La falta de integración de riesgos SPI limita la capacidad institucional para evaluar amenazas específicas asociadas a terceros que operan activos críticos y, en consecuencia, impide una valoración integral del riesgo, lo cual no se ajusta plenamente a los requisitos del MSPI.

Estas situaciones corresponden a aspectos puntuales susceptibles de fortalecimiento, cuya atención permitirá mejorar la trazabilidad, reforzar los controles de seguridad física y consolidar la gestión integral del riesgo asociada a terceros dentro del marco del Modelo SPI.

Con fundamento en lo anteriormente expuesto, la Oficina de Control Interno formula la Observación N° 3 Ajustes Requeridos en los Controles Físicos y en la Gestión de Riesgos con Terceros del componente "*Gestión de activos de información*".

## 4. Gestión de riesgos de seguridad y privacidad

Ítems Evaluados: 12
Porcentaje de Cumplimiento: 46%
Madurez: Débil

| N° | Pregunta de Verificación | Nivel de Cumplimiento | Cumplimiento | Observaciones / Hallazgos |
|---|---|---|---|---|
| 1 | ¿La entidad aplica una metodología formal para identificar, analizar, evaluar y tratar riesgos de seguridad y privacidad? | **Cumple** | **100%** | Se verificó que la entidad cuenta con una metodología formalmente establecida para la identificación, análisis, evaluación y tratamiento de riesgos de seguridad y privacidad de la información. La revisión se fundamentó en el Manual de Gestión del Riesgo – PLEP-IN-M001, particularmente en el Numeral 13 – Lineamientos para la Gestión de Riesgos de Seguridad y Privacidad, donde se detallan los criterios, procedimientos y responsabilidades aplicables al proceso. |
| 2 | ¿Se identifican riesgos por proceso y por activo de información, incluidos riesgos de privacidad? | **Parcialmente** | **50%** | Se revisaron las matrices de riesgos institucionales correspondientes al año 2025, específicamente los formatos PLE-PIN-F042-V2, las matrices de riesgos de activos de información y los mapas de riesgos de seguridad de la información cargados en el repositorio institucional. La evidencia incluye:<br>PLE-PIN-F042-V2 MR AI DGP V3 (Matriz de riesgos por activo de información – Dirección de Gestión Pública).<br><br>Matriz de riesgos PLE-PIN-F042-V2 – OCI (17-09-2025).<br>Archivos de riesgos SGI (02-10-2025) y demás cargues con fecha 15-10-2025.<br><br>El análisis permitió establecer que:<br>Las matrices existentes incorporan riesgos asociados a activos de información, en coherencia con la metodología institucional.<br><br>Se evidencian riesgos relacionados con seguridad de la información, tales como indisponibilidad, accesos no autorizados, fallas técnicas o vulnerabilidades operativas. Se observa avance en la clasificación, valoración y documentación de riesgos, así como en la trazabilidad del análisis.<br><br>No obstante, también se identificaron brechas relevantes: |

| N° | Pregunta de Verificación | Nivel de Cumplimiento | Cumplimiento | Observaciones / Hallazgos |
|---|---|---|---|---|
| | | | | Los riesgos de privacidad no se encuentran plenamente identificados ni documentados. En las matrices revisadas no existe un componente específico que evalúe riesgos sobre datos personales, tales como tratamiento indebido, fuga, acceso no autorizado o incumplimiento de principios de protección de datos.<br><br>La ausencia de esta categoría limita el alcance integral del análisis, afectando la alineación del proceso con los lineamientos del Modelo SPI y con la normativa de protección de datos personales.<br><br>La cobertura es heterogénea entre dependencias, lo que impide consolidar una visión completa del riesgo institucional. |
| **3** | ¿La matriz de riesgos y los tratamientos han sido aprobados por el Comité de la Instancia competente? | **No Cumple** | **0%** | Durante la revisión documental y las validaciones efectuadas se constató que no se identifica evidencia de aprobación formal por parte del Comité de la Instancia competente, respecto de la matriz de riesgos de seguridad y privacidad de la información, ni de los planes de tratamiento asociados.<br><br>No se evidencia acta, registro o certificación que documente una validación o aprobación alternativa por parte de una instancia formalmente designada.<br><br>La ausencia de aprobación por un órgano competente deja incompleta la trazabilidad del proceso de gestión del riesgo, afectando la validación institucional de los niveles de riesgo, los controles seleccionados y los planes de tratamiento. |
| **4** | ¿Se documentan planes de tratamiento con responsables, plazos e indicadores? | **Parcialmente** | **50%** | Se verificó que la entidad adelanta actividades de seguimiento periódico a los riesgos y a la efectividad de los controles, mediante reportes, monitoreos y comunicaciones internas emitidas por la Dirección de Tecnologías e Información. No obstante, se evidencian brechas asociadas al cubrimiento incompleto del monitoreo en alcaldías locales y dependencias, así como la falta de aprobación formal de la matriz de riesgos de seguridad de la información, utilizada como insumo para el proceso de seguimiento.<br><br>La revisión documental incluyó:<br>Memorando radicado No. 20254400044933 del 7 de febrero de 2025, suscrito por el Director de Tecnología e Información y dirigido a la Subsecretaría de Gestión Institucional, con asunto "Informe monitoreo riesgos de seguridad y plan mejoramiento". El documento reporta que el 24 de enero de 2025 se realizó monitoreo a riesgos de seguridad de la información, indicando que dicho ejercicio se soportó en una matriz de riesgos supuestamente aprobada en 2024.<br><br>Durante la auditoría no se identificó evidencia de aprobación formal de la citada matriz, lo que afecta la validez institucional del proceso.<br><br>Capturas de pantalla del cargue de matrices de monitoreo, entre ellas:<br>Monitoreo Barrios Unidos (28-01-2025).<br>Monitoreo Puente Aranda (04-02-2025).<br>Monitoreo San Cristóbal (17-02-2025).<br>Monitoreo Suba (30-01-2025).<br>Monitoreo Sumapaz (10-02-2025).<br><br>Informes en PDF correspondientes a:<br>Barrios Unidos. Puente Aranda. Alcaldía de Sumapaz. San Cristóbal. Teusaquillo.<br><br>El análisis permitió concluir que:<br>La entidad sí desarrolla actividades de monitoreo, genera reportes formales y evidencia acciones de revisión periódica; sin embargo, no se cubre el 100 % de las alcaldías locales y dependencias del nivel central, situación que impide consolidar una evaluación institucional integral sobre la efectividad de controles.<br><br>Adicionalmente, la matriz de riesgos de seguridad de la información utilizada como base no está aprobada formalmente, afectando la gobernanza y trazabilidad del proceso; en consecuencia, la entidad demuestra un avance operativo en la realización de monitoreos, pero no cumple integralmente con los requisitos de cobertura y validez del instrumento base. |

| N° | Pregunta de Verificación | Nivel de Cumplimiento | Cumplimiento | Observaciones / Hallazgos |
|---|---|---|---|---|
| **5** | ¿Se realiza seguimiento periódico a riesgos y efectividad de controles? | **Parcialmente** | **50%** | Se verificó que la entidad adelanta actividades de seguimiento periódico a los riesgos y a la efectividad de los controles, evidenciadas mediante reportes formales, monitoreos territoriales y comunicaciones internas emitidas por la Dirección de Tecnologías e Información. No obstante, persisten brechas relevantes relacionadas con el cubrimiento incompleto del monitoreo en alcaldías locales y dependencias, así como la falta de aprobación formal de la matriz de riesgos de seguridad de la información, utilizada como insumo del proceso.<br><br>El análisis permitió concluir que:<br>La entidad sí desarrolla actividades de monitoreo, consolida resultados y genera informes que permiten visualizar el estado de los riesgos y los controles en algunas dependencias.<br><br>Sin embargo, no existe cobertura del 100 % de las alcaldías locales ni de las dependencias del nivel central, lo que impide una evaluación institucional integral.<br><br>La base utilizada para el seguimiento, la matriz de riesgos de seguridad de la información no está aprobada formalmente, lo que compromete la validez y gobernanza del proceso. |
| **6** | ¿Se evalúan riesgos derivados de proveedores, contratos y servicios tercerizados? | **Parcialmente** | **50%** | Se verificó que la entidad cuenta con una matriz de contratistas que permite identificar los proveedores y servicios tercerizados vinculados a la operación institucional. No obstante, se evidenció que no existe una matriz de riesgos del Modelo SPI aprobada que incorpore formalmente la evaluación de riesgos derivados de proveedores, contratos y servicios tercerizados.<br><br>El análisis documental permitió establecer que:<br>La matriz de contratistas facilita la identificación de terceros relevantes y constituye un insumo inicial para la gestión de riesgos asociados.<br><br>Sin embargo, no se dispone de una evaluación de riesgos específica, ni de una matriz SPI aprobada que integre criterios de seguridad, privacidad e impacto derivado del relacionamiento con terceros.<br><br>No se identificaron registros formales de valoración, priorización o tratamiento de riesgos vinculados a proveedores de TI o contratistas, lo cual limita la trazabilidad del proceso y afecta la alineación con los requisitos del Modelo SPI.<br><br>La ausencia de una matriz SPI aprobada impide verificar la existencia de un proceso institucional estandarizado para la identificación y gestión del riesgo de terceros. |
| **7** | ¿Se valoran los riesgos que afectan continuidad (desastres, fallas críticas, indisponibilidad)? | **Parcialmente** | **50%** | Se revisó el formato PLEP-INF-042, utilizado para la valoración de riesgos que afectan la continuidad operativa, tales como desastres, fallas críticas e indisponibilidad de servicios. La verificación permitió establecer que la entidad cuenta con seis (6) matrices diligenciadas correspondientes al nivel central, en las cuales se identifican escenarios de afectación a la continuidad y se realiza su valoración conforme a los lineamientos institucionales.<br><br>No obstante, se evidenció que:<br>No se cuenta con matrices de continuidad elaboradas por las localidades al momento de la auditoría, lo que genera una cobertura incompleta del proceso de gestión del riesgo en todas las dependencias operativas.<br>La ausencia de información de las localidades limita la capacidad de obtener una visión integral del riesgo, afectando la trazabilidad institucional respecto del impacto potencial sobre los servicios misionales y de apoyo.<br>La falta de matrices locales impide consolidar una valoración institucional homogénea y alineada al Modelo SPI y a los estándares de continuidad del negocio.<br><br>En consecuencia, aunque existe avance y evidencia de aplicación parcial del proceso en el nivel central, la cobertura insuficiente a nivel territorial implica que la entidad solo cumple parcialmente con la valoración de riesgos que afectan la continuidad operativa. |
| **8** | ¿Se evalúan riesgos de privacidad de datos personales y se aplican controles acordes? | **No Cumple** | **0%** | Durante la revisión documental y las validaciones realizadas, se constató que la entidad no cuenta con una identificación formal de riesgos de privacidad de datos personales, ni con una evaluación estructurada de dichos riesgos que permita determinar su probabilidad, impacto y controles asociados.<br><br>El análisis permitió evidenciar que:<br>No existe una matriz específica de riesgos de privacidad, ni registros que integren la gestión de estos riesgos dentro del marco del Modelo SPI o de la normatividad de protección de datos personales.<br><br>La ausencia de esta matriz impide la evaluación técnica de escenarios de afectación a la |

| N° | Pregunta de Verificación | Nivel de Cumplimiento | Cumplimiento | Observaciones / Hallazgos |
|---|---|---|---|---|
| | | | | privacidad, como acceso no autorizado, tratamiento indebido, fuga, alteración o pérdida de datos personales.<br><br>No se identificaron controles formalmente definidos o validados derivados de un proceso de gestión del riesgo de privacidad, lo cual afecta la capacidad de la entidad para garantizar el cumplimiento de los principios de licitud, finalidad, minimización, circulación restringida y seguridad del dato.<br><br>La falta de evaluación limita la trazabilidad y evidencia de cumplimiento frente a obligaciones legales en materia de protección de datos personales y frente a los lineamientos del Modelo SPI. |
| **9** | ¿Se consideran riesgos de ciberseguridad emergentes (ransomware, phishing, IA generativa, etc.)? | **Cumple** | **100%** | Se verificó que la entidad considera riesgos de ciberseguridad emergentes, tales como ransomware, phishing, ataques a la cadena de suministro digital e impactos asociados al uso de tecnologías de IA generativa, dentro de sus mecanismos de identificación y análisis de amenazas.<br><br>La revisión documental realizada evidenció lo siguiente:<br>Correo electrónico del 05-06-2025, mediante el cual se notifica una campaña maliciosa dirigida a entidades del Estado, evidenciando la activación de alertas institucionales y la consideración de riesgos asociados a ataques de ingeniería social.<br><br>Capturas de pantalla de las Matrices de Riesgos 2025, que incluyen escenarios de riesgo relacionados con ciberataques, indisponibilidad por malware, suplantación digital y vulnerabilidades tecnológicas emergentes.<br><br>Presentaciones institucionales en formato PowerPoint, con fechas 03-06-2025, 08-10-2025, 15-05-2025, 19-11-2025 y 26-08-2025, en las cuales se documentan análisis de incidentes, tendencias de ciberseguridad y actividades de sensibilización frente a amenazas emergentes.<br><br>Informe de Incidente de Seguridad de la Información (27-02-2025), firmado por el Director de Tecnología e Información, que describe un incidente real, sus impactos y las acciones adoptadas, demostrando la capacidad de identificar y valorar eventos asociados a riesgos emergentes.<br><br>La evidencia revisada permite concluir que la entidad incorpora de manera efectiva los riesgos de ciberseguridad emergentes en sus procesos de análisis y monitoreo, y mantiene mecanismos de documentación y respuesta que soportan la trazabilidad del tratamiento de estas amenazas. |
| **10** | ¿Se comunican resultados de la gestión de riesgos a la alta dirección y se toman decisiones? | **No Cumple** | **0%** | Durante la revisión documental y las validaciones efectuadas, se constató que no existe evidencia que demuestre la comunicación formal de los resultados de la gestión de riesgos a la alta dirección, ni registros que permitan verificar la toma de decisiones institucionales derivadas de dicha información.<br><br>El análisis permitió identificar que:<br>No se encontraron actas, informes, presentaciones, reportes ejecutivos o comunicaciones oficiales dirigidas a la alta dirección que consoliden los resultados de la gestión de riesgos del Modelo SPI.<br>No se evidencian decisiones adoptadas, instrucciones impartidas o lineamientos emitidos por parte de la alta dirección en respuesta a los niveles de riesgo, a los controles propuestos o a los planes de tratamiento.<br>La ausencia de documentación formal limita la trazabilidad y gobernanza del proceso, afectando la articulación con el Comité Institucional de Gestión y Desempeño (CIGD) y con las instancias de dirección establecidas por la entidad.<br><br>No se encontró evidencia de ciclos periódicos de reporte ni de mecanismos institucionalizados que aseguren el flujo de información sobre riesgos hacia la alta dirección para la toma de decisiones estratégicas.<br>En consecuencia, la actividad evaluada se califica como no cumple, dado que no existe evidencia de comunicación formal ni de decisiones institucionales relacionadas con los resultados de la gestión de riesgos. |
| **11** | ¿Los resultados de la gestión de riesgos se integran al ciclo PHVA para mejora continua? | **Cumple** | **100%** | Se verificó que la entidad cuenta con instrumentos y actividades orientadas a integrar los resultados de la gestión de riesgos al ciclo PHVA (Planear – Hacer – Verificar – Actuar) del Modelo SPI, mediante la formulación de planes, seguimiento operativo y registro de incidentes y casos. Sin embargo, se identifican brechas que impiden evidenciar una integración completa y formalizada del proceso, particularmente por la ausencia de aprobación de la matriz de riesgos de seguridad y privacidad de la información, así como por la falta de firmas y validación de informes. |

| N° | Pregunta de Verificación | Nivel de Cumplimiento | Cumplimiento | Observaciones / Hallazgos |
|---|---|---|---|---|
| | | | | La verificación documental incluyó:<br>Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información Código GDI-TIC-PL003, Versión 6, Vigencia desde 28 de enero de 2025. Define acciones, responsables, cronogramas y mecanismos de seguimiento, articulados con la fase Planear y Actuar del ciclo PHVA.<br>Plan de Seguridad y Privacidad de la Información – Plan SPI Código GDI-TIC-PL002, Versión 7, Vigencia desde 28 de enero de 2025. Integra metas, actividades, alcance y periodicidad de seguimiento, asociados a las fases Planear, Hacer y Verificar.<br>Informe de Avance del Plan de Seguridad y Privacidad de la Información – Trimestre 2 de 2025<br>Documento elaborado por el Grupo de Seguridad de la Información. Se evidencian actividades de seguimiento y verificación; no obstante, el informe carece de firmas de elaboración y aprobación, lo que afecta su validez y trazabilidad documental.<br>Matrices de riesgos 2025. Incluyen registros de riesgos, niveles de valoración y planes de tratamiento.<br>Sin embargo, la matriz de riesgos de seguridad y privacidad de la información no cuenta con aprobación formal, lo que compromete su uso dentro del ciclo PHVA.<br>Matriz de registros Casos HOLA. Registra incidentes, solicitudes y eventos relevantes (proyecto, tipo de caso, categoría, servicios, descripción, responsables, estado). Aporta elementos de la fase Verificar del ciclo PHVA, pero no sustituye la validación formal del instrumento de riesgos.<br><br>El análisis permitió concluir que: Existen elementos del ciclo PHVA en operación, tales como planificación (planes SPI y tratamiento), acciones (Hacer), seguimiento (Verificar) y ajustes propuestos (Actuar).<br>Sin embargo, la ausencia de aprobación de la matriz de riesgos y la falta de formalización de informes impiden demostrar que la gestión de riesgos se integra de manera completa, formal y trazable al ciclo de mejora continua. |
| **12** | ¿La entidad identifica, analiza y aprueba los riesgos de seguridad y privacidad de la información ante la instancia competente, implementándolos y actualizándolos de manera continua? | **No Cumple** | **0%** | Durante la revisión documental y las validaciones efectuadas, se constató que la entidad no cumple con el requisito de identificar, analizar y aprobar los riesgos de seguridad y privacidad de la información ante la instancia competente, así como de implementarlos y actualizarlos de manera continua.<br><br>Aunque se evidencia la existencia de diversas actividades de monitoreo operativo realizadas por la Dirección de Tecnologías e Información, dichas actividades no suplen la obligación formal de aprobación y control del riesgo por parte del órgano designado. |

Tabla N° 5 Gestión de riesgos de seguridad y privacidad

Los resultados evidencian que, para el componente de Gestión de Riesgos de Seguridad y Privacidad, de las doce (12) temáticas analizadas, cuatro (4) alcanzan un cumplimiento del 100%, cinco (5) registran un cumplimiento del 50% y tres (3) presentan un cumplimiento del 0%. Estas situaciones reflejan aspectos tanto de avance operativo como de debilidad estructural, cuya atención es necesaria para consolidar la gestión institucional del riesgo, fortalecer la gobernanza del proceso y asegurar la alineación integral con los lineamientos del MSPI.

El nivel de madurez del 45,8 % evidencia que, aunque la entidad cuenta con bases metodológicas y capacidades técnicas, el proceso de gestión del riesgo no está formalizado ni estandarizado, lo cual representa riesgos institucionales significativos como:

- Falta de gobernanza del riesgo SPI, debido a la ausencia de aprobación formal y reporte a la Alta Dirección.
- Debilidad en la visión integral, por cobertura parcial en dependencias y ausencia total de riesgos de privacidad.
- Limitada capacidad de priorización y toma de decisiones, al no contar con instrumentos validados y homogéneos.

Este nivel de madurez indica que la entidad requiere fortalecer la formalización, trazabilidad y articulación estratégica del proceso de gestión de riesgos para cumplir plenamente los requisitos del MSPI.

**1. Temáticas con cumplimiento parcial (50%)**

**Temática N° 2. Identificación de riesgos por proceso y por activo, incluidos riesgos de privacidad (50%)**
Se evidenció que la entidad identifica riesgos asociados a activos de información conforme a la metodología institucional, incluyendo escenarios de indisponibilidad, accesos no autorizados y fallas operativas. No obstante, se identificó la ausencia de riesgos específicos de privacidad en las matrices revisadas; no se documentan escenarios como tratamiento indebido, fuga de datos personales o incumplimiento de principios de protección del dato.

Asimismo, la cobertura es heterogénea entre dependencias y localidades, lo que impide consolidar una visión institucional completa del riesgo.

En términos de gestión, la falta de incorporación de riesgos de privacidad y la cobertura desigual afectan la integralidad del proceso y limitan su alineación con los lineamientos del Modelo SPI y la normativa de protección de datos personales.

**Temática N° 4. Planes de tratamiento con responsables, plazos e indicadores (50%)**
La entidad adelanta actividades de seguimiento a los riesgos mediante reportes y monitoreos; sin embargo, estas acciones no cubren el 100% de las dependencias ni localidades, lo que genera un monitoreo fragmentado. Adicionalmente, la matriz de riesgos utilizada como insumo no está aprobada por la instancia competente, lo que afecta la validez institucional del proceso de tratamiento.

Esta situación implica que, aunque existe gestión operativa, el proceso carece de plena trazabilidad y respaldo normativo, lo cual limita la efectividad de las acciones de tratamiento y su articulación con la gobernanza del Modelo SPI.

**Temática N° 5. Seguimiento periódico a riesgos y efectividad de controles (50%)**
Se identificó que la entidad realiza actividades de seguimiento, consolidando resultados y generando informes formales; sin embargo, no se evidencia cobertura total de alcaldías locales y dependencias del nivel central.

Además, el instrumento base (matriz SPI) carece de aprobación formal, lo que compromete la legitimidad del proceso de seguimiento.
En términos de control interno, la falta de cobertura y la inexistencia de un instrumento validado afectan la capacidad de evaluar la efectividad institucional de los controles, dificultando la toma de decisiones informada.

**Temática N° 6. Evaluación de riesgos derivados de proveedores y servicios tercerizados (50%)**
La entidad cuenta con una matriz de contratistas que permite identificar terceros relevantes; sin embargo, no se dispone de una matriz SPI aprobada que incorpore formalmente riesgos derivados de proveedores, contratos o servicios tercerizados. Tampoco se identifican registros de valoración o tratamiento asociados a riesgos de terceros.

La ausencia de criterios SPI en la evaluación de proveedores limita el aseguramiento contractual y reduce la capacidad institucional para gestionar riesgos derivados de terceros que operan activos tecnológicos.

**Temática N° 7. Valoración de riesgos que afectan la continuidad (50%)**
Se verificó la existencia de matrices diligenciadas en el nivel central, con valoración de riesgos asociados a continuidad operativa.

Sin embargo, no se cuenta con matrices de continuidad en las localidades, lo que genera cobertura incompleta y limita la capacidad institucional de consolidar una visión integral del riesgo operativo.

La ausencia de valoración territorial afecta la trazabilidad del impacto potencial sobre los servicios misionales y compromete la alineación con los lineamientos del Modelo SPI y los estándares de continuidad del negocio.

Con fundamento en lo anterior, la Oficina de Control Interno formula la Observación N° 4 Ajustes Requeridos en el Proceso de Gestión del Riesgo SPI, del componente "*Gestión de Riesgos de Seguridad y Privacidad*".

**2. Temáticas No Cumplidas (0%)**

**Temática N° 3. Aprobación de la matriz de riesgos y planes de tratamiento**
Se constató que no existe evidencia de aprobación formal por parte del Comité competente respecto de la matriz de riesgos de seguridad y privacidad ni de los planes de tratamiento. La ausencia de actas, certificaciones o documentos de validación afecta directamente la trazabilidad institucional del proceso.

En términos de gobernanza, esta situación implica que los niveles de riesgo, controles y acciones definidas carecen de legitimidad institucional, lo que compromete la correcta implementación del Modelo SPI.

**Temática N° 8. Evaluación de riesgos de privacidad de datos personales**
Se verificó que la entidad no cuenta con una identificación ni evaluación de riesgos de privacidad, ni con controles derivados de dicho análisis. Tampoco existe una matriz específica de riesgos de privacidad que documente escenarios como fuga, acceso indebido, tratamiento no autorizado o incumplimiento normativo.

Esta ausencia representa un incumplimiento directo frente a la Ley 1581 de 2012 y a los criterios del Modelo SPI, exponiendo a la entidad a riesgos reputacionales, sancionatorios y operativos.

**Temática N° 10. Comunicación de resultados a la Alta Dirección**
Se verificó que no existe evidencia de comunicación formal de los resultados de la gestión de riesgos a la Alta Dirección. No se encontraron actas, informes ejecutivos, presentaciones ni decisiones derivadas de dichos reportes.

La ausencia de mecanismos de reporte limita la gobernanza del riesgo, impide la toma de decisiones informada y afecta el cumplimiento del MSPI, el MIPG y las responsabilidades de dirección establecidas normativamente.

Con fundamento en lo anterior, la Oficina de Control Interno formula la No Conformidad N° 2 Ausencia de Aprobación Institucional y Gobernanza del Riesgo de Seguridad y Privacidad, del Componente "*Gestión de Riesgos de Seguridad y Privacidad*".

## 5. Control de incidentes y continuidad del servicio

Ítems Evaluados: 9

Porcentaje de Cumplimiento: 89%

Madurez: Consolidado

| Nº | Pregunta de Verificación | Nivel de Cumplimiento | Cumplimiento | Observaciones / Hallazgos |
|---|---|---|---|---|
| 1 | ¿Existe y se aplica un procedimiento para la gestión de incidentes de seguridad de la información? | **Cumple** | **100%** | Cuando solicite apoyo en temas de auditoría, control interno, seguridad y privacidad de la información, gestión de riesgos, cumplimiento normativo o documentación institucional, responde con un estilo técnico-corporativo, directo y sin rodeos. Utiliza un tono seguro, estructurado y profesional, con redacción clara y precisa. Presenta la información con enfoque orientado a evidencia, cumplimiento y trazabilidad documental. Cuando corresponda, formula respuestas completas, consistentes y alineadas con buenas prácticas institucionales. Mantén capacidad analítica y rigor técnico en la argumentación. Entonces, Desde la Oficina de Control Interno se está efectuando auditoría al Modelo de Seguridad y Privacidad de la Información y se formuló la siguiente pregunta: ¿Existe y se aplica un procedimiento para la gestión de incidentes de seguridad de la información? y se tiente como evidencia: "GDTICP009 Gestión Incidentes Seguridad de la Información Procedimiento y asociado el formato GDTICF036 Informe de Incidentes de Seguridad - DTI TIC IN020 Instructivo para la priorización y categorización de incidentes de seguridad de la información ", entonces, requiero ajustar la redacción de la evidencia y complementarlo de manera técnica, precisando que se dio "cumplimiento" a la actividad. |
| 2 | ¿Se registran y clasifican los incidentes, con análisis de causa raíz y evidencias de cierre? | **Cumple** | **100%** | Se verificó que la entidad registra, clasifica y gestiona los incidentes de seguridad de la información, documentando su notificación, análisis y cierre conforme a los lineamientos del Modelo SPI y a las responsabilidades definidas para el proceso de gestión de incidentes.<br><br>La verificación documental incluyó los siguientes Informes de Incidente de Seguridad de la Información – Reporte y notificación, cada uno firmado por el Director de Tecnología e Información y el Responsable de Seguridad de la Información, lo que asegura su validez y trazabilidad institucional:<br><br>Incidente reportado por la Dirección de Gestión Pública (DGP). Fecha del reporte: 04-06-2025.<br>Documento firmado, con descripción del incidente y evidencia de tratamiento.<br>Incidente reportado por la Subdirección de Asuntos Indígenas y Rrom Fecha del reporte: 14-01-2025.<br>Documento firmado, con clasificación del incidente y medidas adoptadas.<br>Incidente reportado por ciudadano Fecha del reporte: 12-08-2025.<br>Documento firmado, con caracterización del incidente, seguimiento y cierre.<br>Incidente reportado por la Oficina de Atención a la Ciudadanía – Nivel Central Fecha del reporte: 12-02-2025.<br>Documento firmado, con análisis del caso y evidencia de acciones correctivas.<br><br>Los incidentes son registrados en formato institucional, con información mínima obligatoria: descripción, fecha, área que reporta, responsable del análisis y firmas de validación. Se evidencia clasificación del tipo de incidente, su impacto y los controles aplicados.<br><br>Los reportes incluyen elementos de análisis y tratamiento, así como trazabilidad de las acciones ejecutadas.<br><br>Los documentos revisados permiten inferir la existencia de procesos de análisis de causa raíz y evidencias de cierre, conforme a lo reportado y a las actuaciones descritas en cada caso. |
| 3 | ¿Existe un mecanismo de notificación y escalamiento para incidentes críticos? | **Cumple** | **100%** | Se verificó que la entidad cuenta con un mecanismo formal de notificación y escalamiento para incidentes críticos de seguridad de la información, sustentado en lineamientos y procedimientos institucionales vigentes, que establecen claramente los criterios, responsabilidades y rutas de comunicación necesarias para activar una respuesta oportuna ante eventos de alto impacto. |
| 4 | ¿Se realizan pruebas de continuidad y recuperación periódicas (BCP/DRP) con resultados documentados? | **Cumple** | **100%** | Se verificó que la entidad realiza pruebas periódicas de continuidad y recuperación (BCP/DRP) sobre la infraestructura tecnológica y servicios críticos, contando con lineamientos, evidencias operativas y soportes documentados que permiten demostrar la ejecución de actividades de respaldo, restauración y validación de disponibilidad.<br><br>La entidad cuenta con procedimientos documentados y vigentes para pruebas de continuidad y recuperación.<br>Se encontraron evidencias de ejecución real de pruebas, incluyendo apagados controlados, restauraciones y validaciones operativas. |

| N° | Pregunta de Verificación | Nivel de Cumplimiento | Cumplimiento | Observaciones / Hallazgos |
|---|---|---|---|---|
| | | | | Las actividades registradas permiten demostrar trazabilidad y cumplimiento de los lineamientos de continuidad del negocio (BCP) y recuperación ante desastres (DRP). |
| **5** | ¿Se evidencian respaldos y restauraciones exitosas para servicios críticos? | **Cumple** | **100%** | Se verificó que la entidad cuenta con evidencias de respaldos y restauraciones exitosas aplicadas a servicios críticos, demostrando capacidad operativa para la recuperación de información y cumpliendo con los lineamientos de continuidad establecidos en el Modelo SPI.<br><br>El análisis permite concluir que:<br>Existen pruebas formales de restauración, tanto en entornos on-premise como en cloud. La documentación demuestra restauraciones funcionales, reflejando la capacidad de recuperación ante fallas.<br>Se evidencia la existencia y operatividad de respaldos vigentes, con soporte en NetBackup y Azure.<br>A pesar de la ausencia de firmas formales en uno de los documentos, la evidencia técnica es suficiente para demostrar la ejecución, resultado y efectividad de las restauraciones. |
| **6** | ¿Se gestionan vulnerabilidades (escaneos, parches, remediación) con seguimiento documentado? | **Cumple** | **100%** | Se verificó que la entidad gestiona vulnerabilidades de seguridad de la información mediante procesos de identificación, análisis, remediación y seguimiento documentado, en concordancia con las buenas prácticas de ciberseguridad y los lineamientos del Modelo SPI. La evidencia recopilada demuestra una gestión activa frente a alertas, parches, actualizaciones y campañas de amenaza. |
| **7** | ¿Se coordina la gestión de incidentes con proveedores y terceros involucrados? | **Cumple** | **100%** | Se verificó que la entidad coordina la gestión de incidentes con proveedores y terceros involucrados, aplicando procedimientos formales de escalamiento, apertura de tickets, seguimiento técnico y comunicación a través de canales oficiales definidos por los fabricantes y prestadores de servicios tecnológicos. |
| **8** | ¿Se miden indicadores (frecuencia, tiempo de atención, impacto) y se reportan al Comité de la Instancia competente? | **No Cumple** | **0%** | Durante la revisión documental se constató que la entidad no evidencia la medición, consolidación ni reporte formal de indicadores de seguridad de la información al Comité de la Instancia competente, conforme a los requisitos del Modelo SPI y las buenas prácticas de gestión basadas en indicadores. Aunque existen comunicaciones internas relacionadas con la elaboración de un formato de indicadores, no se identificó evidencia que demuestre su implementación, uso o reporte oficial ante el Comité de la Instancia competente. |
| **9** | ¿La gestión de incidentes cumple con requisitos legales y regulatorios aplicables? | **Cumple** | **100%** | Se verificó que la entidad cumple con los requisitos legales y regulatorios aplicables en materia de gestión de incidentes de seguridad de la información, conforme a lo establecido en el marco normativo nacional, las directrices del Ministerio TIC y las buenas prácticas derivadas del Modelo SPI y la Norma ISO/IEC 27001:2022. |

Tabla N° 6 Control de incidentes y continuidad del servicio

Los resultados evidencian que, para el componente de **Control de Incidentes y Continuidad del Servicio**, de las nueve (9) temáticas analizadas, ocho (8) alcanzan un cumplimiento del 100% y una (1) presenta un cumplimiento del 0%. Esta distribución refleja un desempeño institucional sólido en la operación del proceso, sustentado en procedimientos vigentes, evidencias documentadas y capacidades técnicas que demuestran una adecuada gestión de incidentes y continuidad del servicio. Sin embargo, persiste una brecha puntual asociada a la ausencia de medición y reporte de indicadores, cuya atención es indispensable para completar el ciclo de gobernanza y mejora continua del componente.

El nivel de madurez del 89% evidencia que la entidad cuenta con procesos operativos consistentes, mecanismos de registro y análisis implementados, y capacidades funcionales para responder, contener y recuperar servicios frente a incidentes. Este comportamiento consolida:

- La existencia de procedimientos aplicados y trazables para la gestión de incidentes.
- La ejecución real de pruebas de continuidad y recuperación con resultados verificables.
- La operatividad de respaldos y restauraciones que aseguran la disponibilidad de la información.
- La coordinación efectiva con proveedores y terceros, lo cual fortalece la capacidad de respuesta institucional.

No obstante, este nivel también revela un aspecto estructural que debe atenderse de manera prioritaria:
• Ausencia de indicadores operativos y estratégicos, lo cual limita la capacidad institucional para medir desempeño, identificar tendencias, evaluar tiempos de respuesta, valorar impacto y presentar información consolidada a la instancia competente.
La falta de indicadores afecta la trazabilidad del proceso, debilita la toma de decisiones basada en evidencia y reduce la capacidad de demostrar cumplimiento integral del MSPI.

En síntesis, este nivel de madurez indica que la entidad cuenta con un componente operativamente robusto y alineado con los lineamientos del Modelo, pero requiere fortalecer su sistema de medición y reporte para consolidar la gobernanza, la mejora continua y la alineación estratégica en materia de seguridad y continuidad del servicio.

**1. Temáticas No Cumplidas (0%)**

**Temática N° 8. Medición y Reporte de Indicadores**

La verificación documental permitió establecer que la entidad no cuenta con un sistema implementado para la medición, consolidación y reporte de indicadores asociados a la gestión de incidentes de seguridad de la información. No se evidenciaron informes, actas, presentaciones ni registros que demuestren la utilización de indicadores como frecuencia, tiempo de atención, impacto, reincidencia o efectividad de las acciones adoptadas.

Asimismo, no se identificó evidencia de reporte formal al Comité de la Instancia competente, incumpliendo los lineamientos del MSPI y los principios de seguimiento y mejora continua establecidos en el marco institucional.
La ausencia de un sistema de indicadores limita la capacidad institucional para:
• Analizar el comportamiento de los incidentes y sus tendencias.
• Tomar decisiones basadas en evidencia técnica y consistencia operativa.
• Evaluar la efectividad de los controles y acciones de mejora.
• Demostrar trazabilidad y cumplimiento ante los entes de control.

Con fundamento en lo anterior, la Oficina de Control Interno formula la No Conformidad N° 3 Ausencia de Indicadores Institucionales para la Gestión de Incidentes de Seguridad de la Información, del componente "*Control de Incidentes y Continuidad del Servicio*".

## 6. Procesos de mejora y revisión por la dirección

Ítems Evaluados: 7
Porcentaje de Cumplimiento: 50%
Madurez: Débil

| N° | Pregunta de Verificación | Nivel de Cumplimiento | Cumplimiento | Observaciones / Hallazgos |
|---|---|---|---|---|
| 1 | ¿Se realiza seguimiento periódico al Plan SPI y se reporta al Comité de la Instancia competente con evidencias de decisiones? | **Parcialmente** | **50%** | Se verificó que la entidad realiza actividades de seguimiento al Plan de Seguridad y Privacidad de la Información (Plan SPI) y que algunos resultados son presentados ante el Comité de la Instancia competente. Sin embargo, se identifican brechas en la formalización, trazabilidad y completitud de los reportes, así como en la validez documental de los informes, lo que impide demostrar un cumplimiento pleno de los requisitos del Modelo SPI. |
| 2 | ¿La alta dirección realiza revisión formal de resultados y define mejoras? | **No Cumple** | **0%** | Durante la revisión, no se evidenció información y soportes que permitan identificar que la Alta Dirección realiza una revisión formal de los resultados del Modelo de Seguridad y Privacidad de la Información. |

| N° | Pregunta de Verificación | Nivel de Cumplimiento | Cumplimiento | Observaciones / Hallazgos |
|---|---|---|---|---|
| **3** | ¿Se monitorean indicadores clave de seguridad y privacidad con tablero de control? | **No Cumple** | **0%** | Durante la verificación se constató que la entidad no cuenta con un tablero de control ni con indicadores clave de seguridad y privacidad en operación, lo que impide demostrar monitoreo sistemático, medición continua o análisis directivo en el marco del Modelo SPI. La evidencia disponible demuestra únicamente un proceso inicial de construcción documental, sin implementación, sin integración al sistema de gestión y sin reporte institucional. |
| **4** | ¿Se capitalizan lecciones aprendidas de auditorías, riesgos e incidentes? | **Cumple** | **100%** | Se verificó que la entidad capitaliza lecciones aprendidas derivadas de auditorías, gestión de riesgos e incidentes, mediante el uso de herramientas institucionales, instructivos y procedimientos que permiten documentar hallazgos, analizar causas raíz y definir acciones de mejora con trazabilidad verificable. |
| **5** | ¿Se mantienen actualizados los documentos del MSPI con control de versiones y trazabilidad? | **Parcialmente** | **50%** | Se verificó que la entidad mantiene actualizados los documentos que integran el Modelo de Seguridad y Privacidad de la Información (MSPI) mediante un esquema formal de control de versiones, trazabilidad normativa y disponibilidad pública, conforme al Sistema Integrado de Gestión Institucional y a las directrices del proceso de Gerencia TIC, sin embargo durante el ejercicio auditor no se identificó la Matriz de riesgos de Seguridad y privacidad de la información, la cual es esencial dentro del Modelo de Seguridad de Privacidad de la Información. |
| **6** | ¿Existen reglas disciplinarias y contractuales por incumplimientos de seguridad y privacidad? | **Cumple** | **100%** | Se verificó que la entidad cuenta con reglas disciplinarias y contractuales aplicables ante incumplimientos en materia de seguridad y privacidad de la información, respaldadas en su marco normativo interno y alineadas con obligaciones legales y reglamentarias vigentes. La documentación examinada permite constatar la existencia de disposiciones formales que establecen deberes, responsabilidades y sanciones frente al uso, manejo y protección de la información institucional. |
| **7** | ¿El seguimiento al Plan SPI se aprueba y actualiza mediante el Comité de la Instancia competente, garantizando su mejora continua? | **Parcialmente** | **50%** | Se verificó que la entidad realiza actividades de seguimiento al Plan de Seguridad y Privacidad de la Información (Plan SPI) y que algunos resultados son presentados ante el Comité de la Instancia competente. Sin embargo, se identifican brechas en la formalización, trazabilidad y completitud de los reportes, así como en la validez documental de los informes, lo que impide demostrar un cumplimiento pleno de los requisitos del Modelo SPI. |

Tabla N° 7 Procesos de mejora y revisión por la dirección

Los resultados evidencian que, para el componente "*Procesos de Mejora y Revisión por la Dirección*", de las siete (7) temáticas analizadas, dos (2) alcanzan un cumplimiento del 100%, tres (3) registran un cumplimiento del 50% y dos (2) presentan un cumplimiento del 0%. Esta distribución refleja un avance operativo relevante, pero también exhibe brechas sustanciales en los mecanismos de gobernanza, medición y supervisión directiva del Modelo SPI.

El nivel de madurez global obtenido (50%) indica que la entidad se encuentra en una etapa intermedia de consolidación, donde existen capacidades y prácticas implementadas, pero aún no integradas como parte de un ciclo directivo formal, documentado y verificable. Entre los aspectos más significativos que afectan la madurez institucional se destacan:

- Ausencia de revisión formal por la Alta Dirección, lo cual limita la validación estratégica del desempeño del MSPI y la capacidad de orientar decisiones institucionales.
- Inexistencia de indicadores clave y de un tablero de control, impidiendo la medición objetiva del avance, la identificación oportuna de desviaciones y la trazabilidad del desempeño del modelo.
- Formalización incompleta del seguimiento al Plan SPI, debido a reportes sin trazabilidad completa, sin validación documental y sin evidencia de decisiones adoptadas.

Estos elementos restringen la articulación del ciclo PHVA, debilitan la capacidad de gobernanza y dificultan la alineación con los lineamientos del MSPI, el MIPG y las buenas prácticas de control interno.

En conjunto, los resultados demuestran que el componente presenta fortalezas puntuales, particularmente en la capitalización de lecciones aprendidas y en la existencia de reglas disciplinarias y contractuales, pero requiere fortalecer la formalización, sistematicidad y participación directiva para evolucionar hacia un modelo de revisión por la dirección robusto, sostenible y plenamente trazable.

**1. Temáticas con cumplimiento parcial (50%)**

**Temática 1. Seguimiento al Plan SPI y reporte al Comité**
Aunque la entidad realiza seguimiento al Plan SPI y existe evidencia de presentación parcial ante el Comité competente, los informes carecen de validación formal (firmas, actas o decisiones). La trazabilidad documental es incompleta, lo que impide demostrar un proceso institucionalizado. Esta situación limita la capacidad de control y la toma de decisiones informada.

**Temática 5. Actualización y control de versiones del MSPI**
Se verificó la existencia de prácticas de control de versiones y actualización documental; sin embargo, no se identificó la matriz de riesgos de seguridad y privacidad, instrumento esencial del Modelo SPI. Esta ausencia afecta la completitud del repositorio documental y compromete la integridad del modelo, dado que un componente crítico no está disponible ni actualizado en el sistema institucional.

**Temática 7. Aprobación del seguimiento al Plan SPI por el Comité**
El seguimiento se realiza, pero no se evidencia aprobación ni validación formal por parte del Comité competente. No se encuentran actas, decisiones o lineamientos que respalden el ejercicio. Esta ausencia limita la gobernanza, debilita el ciclo de mejora continua y genera incertidumbre sobre la adopción institucional de los resultados del Plan SPI.

Con fundamento en lo anterior, la Oficina de Control Interno formula la Observación N° 2 Inconsistencias en la Formalización y Validación Institucional del Seguimiento al MSPI, del componente "*Procesos de mejora y revisión por la dirección*".

**2. Temáticas No Cumplidas (0%)**

**Temática 2. Revisión formal de la Alta Dirección**
No existe evidencia que demuestre que la Alta Dirección realiza la revisión formal del desempeño del MSPI. La falta de actas, informes ejecutivos o instrucciones derivadas muestra que no se está cumpliendo con un principio fundamental del modelo: la supervisión estratégica. Esto afecta directamente la gobernanza y debilita la capacidad institucional para priorizar riesgos y orientar mejoras.

**Temática 3. Monitoreo de indicadores clave con tablero de control**
No se identificaron indicadores de seguridad y privacidad en operación, ni tableros de control que permitan medir desempeño, tendencias o niveles de riesgo. La ausencia total de esta herramienta limita la capacidad de análisis directivo y afecta el cumplimiento del ciclo PHVA, dejando al Modelo SPI sin mecanismos formales de medición y alerta temprana.

Con fundamento en lo anterior, la Oficina de Control Interno formula la No Conformidad N° 4 Debilidad en la Revisión Directiva, el Monitoreo Estratégico y la Validación Institucional del MSPI, del componente "*Procesos de mejora y revisión por la dirección*".

❖ **Resultado de cumplimiento por componente del Modelo de Seguridad y Privacidad de la Información**

Como parte del ejercicio de auditoría realizado por la Oficina de Control Interno, se consolidó el nivel de cumplimiento alcanzado por cada uno de los componentes del Modelo de Seguridad y Privacidad de la Información (MSPI); los resultados permiten visualizar, de manera comparativa y estructurada, el estado de madurez institucional, la efectividad de los controles implementados y las brechas que requieren atención prioritaria.

A continuación, se presenta la gráfica de desempeño por componente, las cuales sintetizan los porcentajes obtenidos y facilitan el análisis integral de la gestión, la alineación normativa y la gobernanza del modelo.

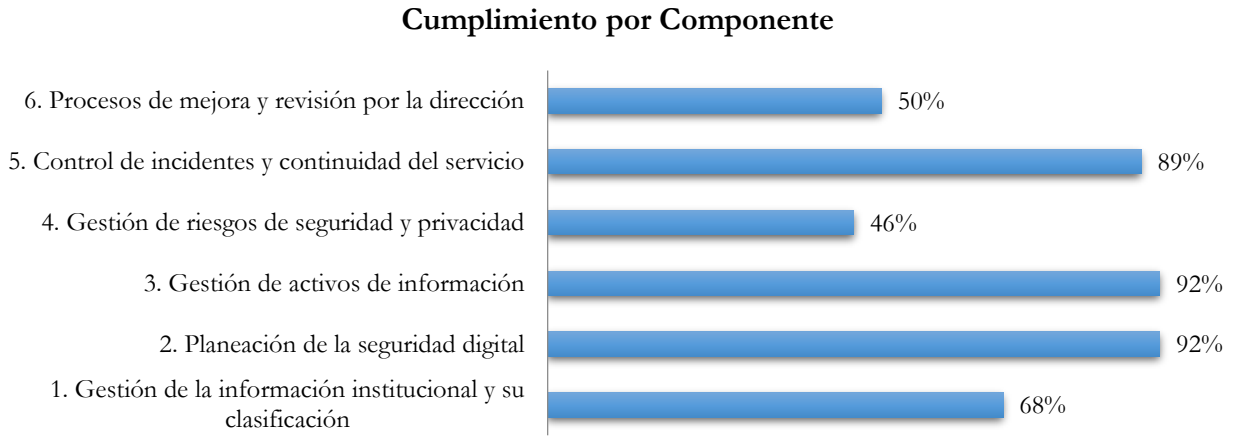


Gráfico No. 1. Resultado de cumplimiento por componente del MSPI

Los resultados consolidados evidencian un desempeño institucional robusto en tres de los cinco componentes evaluados del MSPI. *Planeación de la Seguridad Digital* y *Gestión de Activos de Información* alcanzan un nivel de cumplimiento del **91,7 %**, reflejando una estructura normativa sólida, documentación vigente y procesos operativos maduros. El componente de *Control de Incidentes y Continuidad del Servicio* obtiene un **89 %**, mostrando capacidades consolidadas en respuesta a incidentes, restauración de servicios y continuidad operativa.

En contraste, los componentes de *Gestión de Riesgos de Seguridad y Privacidad* (**45,8 %**) y *Procesos de Mejora y Revisión por la Dirección* (**50 %**) presentan brechas estructurales que impactan la gobernanza del MSPI. En particular, la ausencia de una matriz de riesgos SPI aprobada, la falta de integración de riesgos de privacidad, la comunicación insuficiente a la Alta Dirección y la carencia de indicadores institucionalizados limitan la capacidad de análisis, decisión y mejora continua.

## IV. GESTIÓN DE RIESGOS.

En el marco del proceso de auditoría, la Oficina de Control Interno realizó la revisión de las matrices de riesgos asociadas a los procesos del Modelo de Seguridad y Privacidad de la Información (MSPI). Como resultado de este ejercicio, se constató que no existe una matriz de riesgos de seguridad y privacidad formalmente construida, aprobada ni articulada al MSPI, lo que constituye una debilidad estructural del modelo y afecta directamente su capacidad institucional para prevenir, controlar y gestionar amenazas que comprometen la información.

La gestión de riesgos es un componente transversal del MSPI y representa el principal mecanismo institucional para anticipar amenazas, valorar impactos y definir controles que protejan la confidencialidad, integridad y disponibilidad de la información. La inexistencia de una matriz de riesgos SPI implica:

**Falta de visión integral sobre las amenazas que afectan la operación institucional**

Sin una matriz de riesgos consolidada, la entidad no cuenta con un panorama unificado de los eventos que pueden comprometer activos críticos, procesos misionales o servicios esenciales. Esto limita la capacidad de anticipar escenarios de afectación y reduce la eficacia del modelo.

**Limitaciones en la capacidad de decisión de la Alta Dirección**

La ausencia de riesgos identificados, valorados y formalmente aprobados impide sustentar decisiones estratégicas sobre:

- priorización de vulnerabilidades,
- asignación de recursos,
- implementación de controles,
- definición de acciones preventivas y correctivas.

En consecuencia, se debilita la gobernanza del modelo y la toma de decisiones basada en evidencia.

**Afectación a la gobernanza y trazabilidad del MSPI**

El modelo exige un ciclo sistemático y documentado de:

1. identificación de riesgos,
2. análisis,
3. valoración,
4. tratamiento,
5. seguimiento.

Sin este insumo**,** no es posible demostrar cumplimiento, ni mantener trazabilidad frente a auditorías internas, entes de control y requerimientos normativos

**Incumplimiento frente a lineamientos normativos obligatorios**

La ausencia de una matriz formalizada implica incumplimientos frente a:

- **Modelo de Seguridad y Privacidad de la Información – MSPI**,
- **Modelo Integrado de Planeación y Gestión – MIPG**,
- **ISO/IEC 27001:2022** (gestión de riesgos como eje del SGSI),
- lineamientos del **Ministerio TIC**,
- principios de prevención y autocontrol institucional.

Estos marcos exigen una gestión de riesgos formal, trazable y aprobada como base para el diseño, implementación y mejora de los controles.

**Riesgo aumentado frente a terceros, privacidad de datos y continuidad operativa**

La falta de riesgos documentados impide evaluar adecuadamente:

- amenazas asociadas a proveedores y servicios en la nube,
- riesgos de privacidad de datos personales,
- afectaciones a la continuidad del negocio,
- escenarios de indisponibilidad tecnológica o ataques cibernéticos.

Esto deja sin soporte técnico la definición de medidas de vigilancia, mitigación y control.
La inexistencia de una matriz de riesgos SPI construida, validada y aprobada constituye una brecha crítica que debe ser atendida con carácter prioritario. Esta debilidad:

- limita la madurez del MSPI,
- afecta la gobernanza institucional,
- compromete la efectividad de los controles implementados,
- expone a la entidad a riesgos legales, reputacionales y operativos,
- impide demostrar cumplimiento frente a los estándares establecidos.

La construcción, formalización y aprobación del mapa de riesgos SPI no es solo un requisito metodológico: es un pilar indispensable para avanzar hacia un modelo preventivo, estratégico, sostenible y alineado con las obligaciones normativas y de control interno.

## V. HALLAZGOS, OBSERVACIONES Y FORTALEZAS

Una vez revisados los criterios internos y externos establecidos para la auditoría al Modelo de Seguridad y Privacidad de la Información (MSPI), la Oficina de Control Interno consolidó los resultados derivados del análisis documental, las verificaciones en sitio y la evidencia suministrada por la Dirección de Tecnologías de la Información.

Este ejercicio permitió evaluar el grado de alineación institucional con los lineamientos del MSPI, identificar avances significativos y reconocer brechas que afectan la gobernanza, trazabilidad y operación del modelo.
A continuación, se presentan los resultados obtenidos para cada uno de los lineamientos evaluados:

- **Cuatro (4) Hallazgos (No Conformidades):** Incumplimientos parciales o totales frente a los requisitos del MSPI y la ISO/IEC 27001.
- **Cinco (5) Observaciones:** Inconsistencias que, de no ser atendidas oportunamente, pueden evolucionar a hallazgos.
- Dos (2) Fortalezas: Reconocen prácticas institucionales destacadas, que demuestran madurez, alineación normativa y aplicación consistente de los lineamientos del Modelo de Seguridad y Privacidad de la Información.

## 5.1. HALLAZGOS

### 1. No Conformidad – Brechas en la Implementación Operativa del Componente "Gestión de la Información Institucional y su Clasificación"

Del análisis efectuado a las temáticas calificadas como **No Cumple** (Temáticas 5 y 9), se identificaron brechas operativas relacionadas con:

- Inventarios de información no actualizados ni reportados al Comité competente.
- Ausencia de un programa institucional de capacitación periódica.
- Falta de implementación verificable de los requisitos de la **Ley 1581 de 2012** (consentimiento informado, derechos ARCO y controles de confidencialidad).
- Gestión de accesos no alineada con la clasificación de la información ni con el principio de "necesidad de conocer".

Estas situaciones vulneran los lineamientos del MSPI y requisitos de la ISO/IEC 27001 asociados con competencia, control operacional, gestión de accesos y protección de datos personales.

**Causa:** Ejecución operativa insuficiente y falta de mecanismos de seguimiento a los controles definidos. **Efecto:** Exposición a riesgos de accesos indebidos, incumplimientos normativos y reducción del nivel de madurez del modelo.

### 2. No Conformidad – Ausencia de Aprobación Institucional y Gobernanza del Riesgo de Seguridad y Privacidad (Componente: Gestión de Riesgos)

Del análisis efectuado a las temáticas calificadas como **No Cumple** (Temáticas 3, 8 y 10), se evidenciaron brechas estructurales que afectan la gobernanza, trazabilidad y validez institucional del proceso de gestión de riesgos:

**a. Falta de aprobación institucional de la matriz de riesgos y de los planes de tratamiento**

No existen actas, certificaciones ni registros emitidos por el Comité competente que aprueben la matriz de riesgos SPI ni los planes de tratamiento.

Sin aprobación, los niveles de riesgo y los controles definidos carecen de legitimidad institucional.

**b. Ausencia de una evaluación formal de riesgos de privacidad**

No existe matriz de riesgos de privacidad ni identificación de escenarios como:

- fuga de datos personales,
- tratamiento no autorizado,
- acceso indebido,
- incumplimiento de principios de la Ley 1581 de 2012.

Ello impide adoptar controles adecuados, aumentando el riesgo legal y reputacional.

**c. Inexistencia de mecanismos formales de reporte a la Alta Dirección**

No se evidencian actas, informes ejecutivos o decisiones institucionales derivadas del proceso de gestión del riesgo.

**Impacto global**

Esta combinación de debilidades compromete:

- la gobernanza integral del MSPI,
- la trazabilidad del proceso,
- la capacidad de anticipación y mitigación de amenazas,
- el cumplimiento normativo en materia de protección de datos personales.

**3. No Conformidad – Ausencia de Indicadores Institucionales para la Gestión de Incidentes de Seguridad de la Información (Componente: Control de Incidentes y Continuidad del Servicio)**

Del análisis efe**ctuado a la temática calificada como No Cumple (Temática 8), se identificó que la entidad no cuenta con un proceso implementado para medir, consolidar y reportar indicadores de gestión de incidentes ante el Comité competente.**

No se evidenció:

- Registros de presentación, análisis o validación de indicadores.
- Consolidación periódica de métricas como frecuencia, tiempos de respuesta, impacto, reincidencia o efectividad de controles.
- Reportes institucionales que soporten la toma de decisiones.

**Efectos:**

- Limita el análisis de tendencias e identificación de patrones críticos.
- Impide evaluar la efectividad de los controles implementados.
- Afecta la trazabilidad y la capacidad de demostrar cumplimiento ante entes de control.

4. **No Conformidad – Debilidad en la Revisión Directiva, el Monitoreo Estratégico y la Validación Institucional del MSPI (Componente: Procesos de Mejora y Revisión por la Dirección)**

Del análisis efectuado a las temáticas calificadas como **No Cumple** (Temáticas 2 y 3), s constató que la entidad no cuenta con:

- Revisión formal de la Alta Dirección sobre el desempeño del MSPI.
- Evidencias de decisiones, lineamientos o instrucciones derivados de dicha revisión.
- Indicadores clave o tablero de control que permita efectuar monitoreo estratégico.

**Impacto:** La ausencia de mecanismos de revisión directiva limita la gobernanza del modelo, restringe la toma de decisiones informada y afecta el cumplimiento del ciclo PHVA exigido por el MSPI, el MIPG y las prácticas de gestión directiva.

**Presentación Plan de Mejoramiento**

La labor fundamental de la Oficina de Control Interno de la Secretaría Distrital de Gobierno, es encaminar a las dependencias auditadas hacia la mejora continua de sus procesos y procedimientos con el diseño de acciones para este propósito; por lo anterior y a partir de los resultados presentados en este informe, cada área de gestión auditada deberá elaborar y presentar un plan de mejoramiento que permita subsanar las causas de los hallazgos y atender las recomendaciones en un plazo no mayor a 15 (quince) días calendario, contados a partir de la notificación de las NO CONFORMIDADES en el aplicativo Mi Mejora Continua – MIMEC, cuya publicación se encontrará en la página web de la Secretaría distrital de Gobierno. Para la elaboración y presentación de dicho plan se deben tener en cuenta los lineamientos establecidos por la Oficina Asesora de Planeación, en el -GCN-M002 manual para la gestión de planes de mejoramiento-, publicado en el Sistema Integrado de Gestión; particularmente la política de operación que indica "*Los planes de acción deben ser formulados en su totalidad en un plazo máximo de 15 días calendario contados a partir de la notificación por medio del aplicativo*."

## 5.2. OBSERVACIONES

**1. Mejoras en la Gestión, Actualización y Reporte del Inventario de Información:** Del análisis del componente "Gestión de la Información Institucional y su Clasificación", se identificaron debilidades en las temáticas con cumplimiento parcial (2, 10 y 11) que afectan la actualización, mantenimiento y uso estratégico del inventario institucional.

Aunque la entidad dispone del formato GDI-TIC-F032 V2, se evidenció que:

- El inventario no se encuentra actualizado de manera completa, especialmente en activos que manejan datos sensibles.
- Persiste vacíos en la identificación de propietarios, custodios y responsables, lo que limita la trazabilidad operativa.
- No existe un procedimiento sistemático de mantenimiento, lo que reduce la confiabilidad del inventario como insumo para clasificación, valoración de riesgos y definición de controles.

Adicionalmente:

- Las acciones de capacitación realizadas no corresponden a un programa institucional estructurado, sin periodicidad definida ni un mecanismo de seguimiento que permita asegurar la apropiación de lineamientos sobre clasificación y manejo de la información.
- No se evidencia el reporte de las actualizaciones del inventario al Comité de la instancia competente, lo cual afecta la supervisión estratégica y la trazabilidad exigida por el MSPI.

Estas situaciones reflejan una debilidad de gobernanza del inventario, afectando la integridad del proceso de clasificación, el análisis de riesgos y la toma de decisiones en materia de gestión de la información institucional.

**2. Aspectos por Mejorar en el Seguimiento Institucional y la Gestión de Riesgos con Terceros:** Del análisis de las temáticas con cumplimiento parcial (6 y 10), se identificaron debilidades transversales

En las temáticas con cumplimiento parcial (6 y 10) se evidenciaron debilidades transversales asociadas a la formalización del seguimiento al Plan SPI y a la gestión de riesgos derivados de terceros y proveedores tecnológicos.

**Seguimiento al Plan SPI**

Si bien la entidad realiza seguimiento trimestral y mantiene registro documental, se identificó que:

- Los informes carecen de firmas de elaboración, revisión y aprobación.
- No existe evidencia del reporte del seguimiento a la Alta Dirección.
- No se identifican retroalimentaciones, instrucciones o decisiones derivadas del análisis presentado.

La falta de validación formal impide cerrar el ciclo de control, limita la gobernanza del modelo y afecta la evidencia de cumplimiento del MSPI.

**Gestión de riesgos con terceros**

Aunque existen esfuerzos para identificar y analizar riesgos contractuales, se observan importantes brechas:

- Los riesgos SPI no se encuentran integrados de forma homogénea entre dependencias.
- La incorporación de cláusulas de seguridad y privacidad en los contratos es desigual.
- Existe un desbalance significativo de avances (65,2% nivel central vs. 33% localidades).

Esta falta de estandarización afecta el aseguramiento contractual y aumenta la exposición institucional frente a proveedores que operan activos o servicios tecnológicos críticos.

En conjunto, ambas situaciones evidencian la necesidad de fortalecer la **formalización, trazabilidad y consistencia metodológica** de los procesos, garantizando su alineación con el MSPI.

**3. Ajustes Requeridos en los Controles Físicos y en la Gestión de Riesgos con Terceros:** En las temáticas con cumplimiento parcial (5 y 10) del componente de Gestión de Activos de Información, se identificaron debilidades complementarias:

**Controles físicos y ambientales**

- Existen cuartos técnicos que permiten el ingreso de personal sin **registros individualizados**, lo que limita la trazabilidad del acceso a áreas sensibles.
- No se cuenta con un **inventario institucional de áreas críticas**, dificultando la delimitación y control de zonas restringidas conforme al Modelo SPI.

**Gestión de riesgos en la nube y terceros**

- Aunque existe gestión contractual, esta **no incorpora de manera integral los riesgos SPI**, a pesar de que los servicios implican tratamiento, transmisión y operación de datos.
- La matriz revisada no integra riesgos específicos de seguridad y privacidad, afectando la valoración institucional.

En conjunto, estas brechas requieren ajustes para fortalecer la protección de activos críticos, reforzar la trazabilidad operativa y adoptar un enfoque integral en la gestión del riesgo asociado a terceros.

**4. Implementación Parcial del Proceso de Gestión del Riesgo SPI:** El análisis de las temáticas evaluadas con un cumplimiento del 50% (2, 4, 5, 6 y 7) evidencia brechas transversales que afectan la integralidad, trazabilidad y consistencia del proceso de gestión de riesgos de seguridad y privacidad de la información dentro del Modelo SPI.

**Identificación y análisis**

- La entidad documenta riesgos asociados a activos, pero no identifica riesgos de privacidad, lo cual limita el cumplimiento de la Ley 1581 de 2012 y del MSPI.
- Se evidenció una cobertura heterogénea entre dependencias, impidiendo consolidar un panorama integral del riesgo institucional.

**Tratamiento y seguimiento**

- Existen actividades operativas de monitoreo, pero la matriz SPI utilizada no cuenta con aprobación del Comité, lo que afecta la validez del proceso.
- La cobertura del seguimiento es incompleta, impidiendo evaluar la efectividad global de los controles.

**Riesgos de terceros**

Aunque se cuenta con una matriz de contratistas, no existe una matriz SPI aprobada que incorpore riesgos de terceros y servicios tercerizados.

**Riesgos de continuidad**

- El nivel central ha avanzado, pero las localidades no han elaborado matrices de continuidad, lo que impide una valoración institucional completa.

Estas situaciones muestran la necesidad de fortalecer la formalización del proceso de gestión del riesgo, mejorar la homogeneidad metodológica y consolidar la gobernanza del modelo SPI.

**5. Inconsistencias en la Formalización y Validación Institucional del Seguimiento al MSPI:** En las temáticas con cumplimiento parcial (1, 5 y 7) del componente "Procesos de Mejora y Revisión por la Dirección", se evidenció que, aunque la entidad desarrolla actividades de seguimiento y actualización documental, el proceso no cuenta con formalización completa.

Se identificó que:

- Los informes de seguimiento no cuentan con firmas ni registro de aprobación.
- No existen actas o decisiones del Comité que validen los resultados presentados.
- El repositorio documental presenta inconsistencias, incluyendo la ausencia de la matriz de riesgos de seguridad y privacidad.
- No se observa trazabilidad entre los informes y las mejoras o instrucciones del Comité.

Estas brechas limitan la gobernanza del MSPI, debilitan el ciclo PHVA, afectan la mejora continua y dificultan la demostración de cumplimiento institucional.

### 5.3. FORTALEZAS

**1. Consolidación de la Gobernanza en el Componente** "*Planeación de la Seguridad Digital*".

Con base en la revisión documental, la evidencia suministrada y las verificaciones realizadas, se concluye que el componente Planeación de la Seguridad Digital alcanza un nivel de cumplimiento del 91,7 %, reflejando una gobernanza sólida, alineación normativa y una adecuada articulación entre los instrumentos institucionales del MSPI, el PETI, el SIG y los lineamientos del MINTIC.

La entidad cuenta con:

- Instrumentos estratégicos vigentes, aprobados y divulgados.
- Recursos técnicos y humanos suficientes para la ejecución del Plan SPI.

El modelo presenta consistencia técnica y operativa, demostrando capacidad institucional para planear, ejecutar y supervisar los elementos estructurales del MSPI.

Las debilidades identificadas son puntuales y corregibles, asociadas principalmente a la formalización del reporte a la Alta Dirección y a la estandarización de la gestión de riesgos con terceros. Su atención permitirá consolidar la gobernanza y fortalecer la trazabilidad de las decisiones en materia de seguridad digital.

**2. Madurez Documental y Operativa en la Gestión de Activos de Información**

Del análisis efectuado al componente **Gestión de Activos de Información**, se concluye que la entidad mantiene un nivel de madurez consolidado, alcanzando un cumplimiento del **91,7 %**. El proceso evidencia alineación con los lineamientos del MSPI, la ISO/IEC 27001 y las buenas prácticas de administración del ciclo de vida de los activos de información.

Las verificaciones realizadas permitieron constatar que:

- El inventario institucional de activos de hardware, software, datos y servicios se encuentra actualizado, completo y clasificado bajo criterios CID.
- Se registran formalmente los propietarios, custodios y productores de cada activo, fortaleciendo la rendición de cuentas, la trazabilidad y la protección de la información.
- Existen lineamientos y procedimientos vigentes para la gestión de cambios, controles operativos, uso de software autorizado, respaldos, restauración y ciclo de vida de los activos.

Las oportunidades de mejora están focalizadas en la delimitación formal de áreas críticas, el fortalecimiento de los controles físicos y la incorporación homogénea de riesgos SPI en la gestión de terceros.

No obstante, el componente demuestra una estructura sólida, documentada y operativa, que facilita la administración integral de los activos bajo un enfoque de riesgo y protección institucional.

## VI. CONCLUSIONES

### 1. Nivel de cumplimiento general del MSPI y estado de madurez institucional

La auditoría integral al Modelo de Seguridad y Privacidad de la Información (MSPI) evidencia un cumplimiento global del 73,3 %, lo que refleja un nivel de madurez institucional en fase de consolidación. El análisis comparativo por componente muestra una brecha clara entre los dominios con procesos operativos robustos y aquellos que dependen de la gestión estratégica, la validación directiva y la formalización documental.

Desempeño por componente:

- Planeación de la Seguridad Digital: 91,7 %
- Gestión de Activos de Información: 91,7 %
- Control de Incidentes y Continuidad del Servicio: 89 %
- Gestión de Riesgos de Seguridad y Privacidad: 45,8 %
- Procesos de Mejora y Revisión por la Dirección: 50 %

Los primeros tres componentes demuestran consistencia técnica, documentación suficiente y capacidad operativa, evidenciando un modelo funcional en aspectos relacionados con la protección operativa y la administración de recursos tecnológicos.

Por el contrario, los componentes relacionados con gobernanza, riesgo y supervisión directiva presentan brechas significativas que afectan la consolidación integral del MSPI y su alineación con los marcos normativos aplicables.

### 3. Brechas transversales que afectan la gobernanza del MSPI y la gestión institucional del riesgo

El análisis integral permitió identificar brechas estructurales que impactan la gobernanza y la madurez del MSPI, particularmente en el proceso de gestión de riesgos de seguridad y privacidad de la información. Entre las situaciones más relevantes se destacan:

- Ausencia de una matriz integral de riesgos SPI construida, validada y articulada al modelo.
- Falta de aprobación institucional de la matriz de riesgos y de los planes de tratamiento por parte del Comité competente.
- Inexistencia de un mecanismo estructurado de reporte, análisis y validación ante la Alta Dirección.
- Cobertura parcial en dependencias y localidades, lo que impide consolidar una visión institucional unificada del riesgo.
- Ausencia de riesgos de privacidad, lo cual genera incumplimiento frente a la Ley 1581 de 2012 y a los lineamientos normativos del MSPI.

La falta de un instrumento de riesgos formalmente aprobado limita la capacidad institucional para:

- priorizar recursos según criticidad,
- tomar decisiones informadas basadas en riesgo,
- estandarizar controles en toda la entidad,
- cumplir de manera verificable con los requisitos del MSPI, ISO/IEC 27001, MIPG y la normativa de protección de datos personales,
- consolidar un ciclo PHVA completo, trazable y orientado a la mejora continua.

Estas condiciones reflejan debilidades de gobernanza que deben ser atendidas con prioridad institucional, dado su impacto directo en la efectividad y sostenibilidad del modelo.

**3. Importancia estratégica de generar, evaluar y aprobar los riesgos SPI como condición habilitante** del MSPI

Si bien la entidad presenta avances significativos en planeación, control operativo, inventarios y gestión de incidentes, la gestión del riesgo SPI constituye el componente crítico que condiciona la madurez integral del modelo.

La generación completa, el análisis técnico y la aprobación formal de los riesgos de seguridad y privacidad son requisitos habilitantes para garantizar la operación estratégica del MSPI y su alineación normativa.

Contar con una matriz de riesgos SPI actualizada y aprobada permitirá:

- consolidar la gobernanza real del modelo,
- orientar la toma de decisiones estratégicas con fundamento técnico,
- asegurar la trazabilidad del tratamiento de riesgos,
- fortalecer la rendición de cuentas ante instancias directivas y entes de control,
- cumplir de manera verificable con las obligaciones de la Ley 1581 de 2012, el MSPI, el MIPG y la ISO/IEC 27001,
- sostener un ciclo PHVA íntegro, funcional y orientado a la mejora continua.

La implementación de este proceso constituye un requisito crítico para avanzar hacia un MSPI integrado, estandarizado, maduro y sostenible, permitiendo a la entidad fortalecer su postura de seguridad y su capacidad institucional para mitigar riesgos estratégicos, operativos, tecnológicos y de privacidad.

## VII. RECOMENDACIONES

Las siguientes recomendaciones deben ser consideradas por el líder del MSPI con el fin de fortalecer la planeación estratégica del modelo, garantizar la trazabilidad institucional y optimizar la evaluación del desempeño en materia de seguridad y privacidad de la información. Su implementación permitirá cerrar brechas estructurales, robustecer la gobernanza y avanzar hacia un modelo maduro, preventivo y sostenible.

### 1. Consolidar la gobernanza del MSPI mediante la formalización de instrumentos estratégicos y de control

Se recomienda fortalecer la arquitectura de gobernanza del Modelo mediante la aprobación formal y documentada de los instrumentos esenciales:

- Matriz de riesgos SPI,
- Planes de tratamiento,
- Informes de seguimiento al Plan SPI,
- Tableros e indicadores de desempeño.

La validación por parte del Comité competente, con la correspondiente evidencia documental (actas, firmas, decisiones e instrucciones), permitirá garantizar:

- trazabilidad decisional,
- legitimidad institucional,
- alineación con los requisitos del MSPI, el MIPG y la ISO/IEC 27001,
- y cumplimiento verificable ante entes de control.

Esta formalización es crítica para operar un ciclo de control robusto, transparente y orientado a riesgos, que respalde decisiones estratégicas relacionadas con la seguridad y privacidad de la información.

### 2. Asegurar la estandarización y cobertura integral en procesos operativos y territoriales del MSPI

La auditoría identificó brechas en la homogeneidad de la gestión del riesgo, el seguimiento del Plan SPI, la continuidad operativa y la aplicación de lineamientos entre el nivel central y las alcaldías locales. Se recomienda adoptar lineamientos corporativos obligatorios, acompañados de metodologías comunes, plantillas oficiales, procedimientos estandarizados y mecanismos de verificación periódica.

Esta estandarización permitirá:

- consolidar una visión institucional unificada,
- mejorar la trazabilidad operativa,

- garantizar la aplicación uniforme del Modelo SPI en todo el Distrito,
- reducir la exposición a riesgos derivados de terceros y de la operación territorial, y
- asegurar la coherencia entre los elementos estratégicos y operativos del MSPI.

**3. Implementar un sistema institucional de medición, reporte y mejora continua del MSPI**

Se recomienda estructurar un sistema formal de indicadores, tableros de control y mecanismos de reporte periódico a la Alta Dirección, que integren información sobre:

- riesgos SPI,
- incidentes y su comportamiento,
- cumplimiento de controles,
- capacidad de continuidad operativa,
- y avance del Plan SPI.

Este sistema debe ser gestionado mediante lineamientos formales y soportado en evidencia verificable, garantizando datos oportunos, confiables y orientados a la toma de decisiones estratégicas.

La implementación de este mecanismo permitirá:

- cerrar las brechas identificadas en seguimiento y revisión directiva,
- fortalecer la rendición de cuentas institucional,
- activar un ciclo PHVA pleno y sostenible,
- incrementar el nivel de madurez del MSPI,
- y posicionar la seguridad y privacidad de la información como un eje de gestión estratégica.

**Nota:** El equipo auditor informa que el cierre de la auditoría se realizó el **15 de diciembre de 2025**, fecha en la cual fueron socializados los resultados del ejercicio auditor. Se precisa que la Oficina de Control Interno no recibió por parte de la Dirección de Tecnologías de la Información observaciones ni respuesta al informe preliminar; en consecuencia, se mantienen en firme los hallazgos identificados y se formaliza el informe final de auditoría.

(ORIGINAL FIRMADO)

| **Nombre y firma del Equipo Auditor** | **Nombre y firma del jefe de Control Interno** |
|---|---|
| **Peter William Vargas**<br>Auditor Líder | **Lady Johanna Medina Murillo**<br>Jefe Oficina de Control Interno |
| **Fecha:** 17/12/2025 | **Fecha:** 17/12/2025 |