I. IDENTIFICACIÓN DE LA AUDITORÍA	
Auditor(es)	1. Sleyna Vásquez Rodríguez 2. Oscar Alberto Barragán León 3. Héctor Darío Triana 4. Yesid Hernando Marín Corba
Proceso o área a auditar	Gobierno y Seguridad Digital
Código PAA / Dependencia	33 - Auditoría a la Política de Seguridad Digital
Objetivo General	Evaluar la política de seguridad digital de la SED, verificando las capacidades institucionales para identificar, gestionar, tratar y mitigar riesgos de seguridad digital conforme al Modelo de Seguridad y Privacidad de la Información (MSPI) (Resolución MinTIC 500/2021) actualizado con la Resolución 02277 del 3 de junio de 2025, así como la implementación de instrumentos de resiliencia, recuperación y respuesta alineados con ISO/IEC 27001:2022 y normatividad asociada.
Alcance	La auditoría abarcó: • Realizar seguimiento a los planes de mejoramiento resultado de la auditoría PAA 2025: 28 - Auditoría Gobierno y Seguridad Digital – Conectividad - Oficina de Tecnologías de la Información y las Comunicaciones – OTIC. • Realizar seguimiento al reporte anual del FURAG 2024, para la política de seguridad digital y el índice I14 de seguridad de la información de la Política de Gobierno Digital. • Revisar el estado de implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, el avance del Plan de Seguridad y Privacidad de la Información - PSPI, así como los controles de la norma ISO 27001:2022 y normatividad asociada. El periodo auditado comprendió del 1 de abril de 2025 al 28 de febrero de 2026.

II. RESULTADOS

2.1. Listado de abreviaturas

- CICCI: Comité Institucional de Coordinación de Control Interno
- CTD: Centro de Tecnologías de Datos
- DAFP: Departamento Administrativo de la Función Pública
- DKIM: DomainKeys Identified Mail
- DMARC: Domain-based Message Authentication, Reporting and Conformance
- FURAG: Formulario Único de Reporte de Avance a la Gestión
- GAP: Análisis de Brechas
- ISO: International Organization for Standardization

- ISOLUCION: Sistema de Gestión Institucional
- MECI: Modelo Estándar de Control Interno
- MinTIC: Ministerio de Tecnologías de la Información y las Comunicaciones
- MIPG: Modelo Integrado de Planeación y Gestión
- MSPI: Modelo de Seguridad y Privacidad de la Información
- NIST CSF: National Institute of Standards and Technology – Cybersecurity Framework
- OCI: Oficina de Control Interno
- OTIC: Oficina de Tecnologías de la Información y las Comunicaciones
- OWASP: Open Web Application Security Project
- OSSTMM: Open Source Security Testing Methodology Manual
- PAA: Plan Anual de Auditoría
- PESI: Plan Estratégico de Seguridad y Privacidad de la Información
- PHVA: Planear, Hacer, Verificar y Actuar
- PM: Plan de Mejoramiento
- PSPI: Política de Seguridad y Privacidad de la Información
- SCI: Sistema de Control Interno
- SED: Secretaría de Educación del Distrito
- SGSI: Sistema de Gestión de Seguridad de la Información
- SIEM: Security Information and Event Management
- SoA: Statement of Applicability (Declaración de Aplicabilidad)
- SPF: Sender Policy Framework
- TIC: Tecnologías de la Información y las Comunicaciones
- UPS: Uninterruptible Power Supply
- XDR: Extended Detection and Response

En el marco de la Auditoría a la Política de Seguridad Digital de la Secretaría de Educación del Distrito – SED, y en cumplimiento del Plan Anual de Auditoría PAA 2026, aprobado por el Comité Institucional de Coordinación de Control Interno (CICCI), la Oficina de Control Interno, en su rol de tercera línea de defensa, desarrolló la evaluación independiente a la Política de Seguridad y Privacidad de la Información PSPI, conforme a los lineamientos del Modelo Integrado de Planeación y Gestión MIPG y a la normativa vigente en materia de control interno, verificando las capacidades institucionales para identificar, gestionar, tratar y mitigar riesgos de seguridad digital, de acuerdo con el MSPI adoptado mediante la Resolución MinTIC 500 de 2021 y actualizado por la Resolución 02277 de 2025, así como la implementación de instrumentos de resiliencia, recuperación y respuesta alineados con la norma ISO 27001:2022 y la normatividad asociada.

Esta evaluación se ajusta al análisis de la Política de Seguridad Digital y de los instrumentos que la desarrollan, incluyendo el seguimiento a planes de mejoramiento, el reporte FURAG y el estado de implementación del MSPI, el PSPI y los controles de la ISO 27001:2022.

El objetivo de la presente auditoría es exclusivamente la evaluación de la Política de Seguridad y Privacidad de la Información de la SED. Por tanto, esta auditoría no incluye la evaluación de la OTIC, ni de otras actividades, procesos, funciones, gestión operativa, administración de riesgos o controles propios de dicha dependencia.

2.2. Estado de implementación del Modelo de Seguridad y Privacidad de la información MSPI y Plan de Seguridad y Privacidad de la Información PSPI

Mediante radicado I-2026-30927 dirigido a la Oficina de Tecnologías de la Información y las Comunicaciones OTIC, se solicitó información inicial sobre el estado de implementación del MSPI, recibiendo respuesta con radicado número I-2026-39982, sobre el cual fue necesario solicitar información adicional con radicado No. I-2026-48840, el cual fue atendido con el memorando No. I-2026-51346.

Con fundamento en la revisión documental, entrevistas efectuadas y análisis de evidencias suministradas por la OTIC, se evaluó el estado de implementación del MSPI, conforme a lo establecido en la Resolución MinTIC 500 de 2021, actualizada por la Resolución 02277 de 2025, y su alineación con la norma ISO 27001:2022.

El MSPI en la SED presenta un nivel de implementación intermedio, con avances en la fase de planificación y operación, sin embargo, se evidenciaron brechas importantes en el cierre del ciclo PHVA, particularmente en actualización normativa, formalización de controles ISO 27001:2022, medición del desempeño y evidencia efectiva de algunos procesos críticos.

Si bien la entidad cuenta con elementos estructurales del SGSI, éstos no se encuentran plenamente consolidados ni actualizados frente a los requerimientos vigentes del MSPI y la versión 2022 de la norma ISO 27001:2022.
A continuación, se presenta un análisis por fases del MSPI.

2.21. Fase de diagnóstico

Durante la auditoría se evidenció que la OTIC manifestó haber realizado el autodiagnóstico del MSPI para la vigencia 2025 a través de la herramienta dispuesta por el MinTIC, basada en ISO 27001:2022.

Una vez revisada la evidencia aportada por el área se constató que cumple en términos generales. Está estructurado por cláusulas 4-10 de ISO 27001:2022 y por controles del Anexo A (A.5-A.8). Incluye evidencias, brechas y recomendaciones por requisito/control. Usa una escala de madurez coherente (Inicial → Optimizado). Presenta indicadores de avance y contraste con NIST CSF. Sin embargo, se identifican brechas en la formalización, automatización y revisión periódica que afectan el cumplimiento del 100%.

2.2.2. Fase de planificación

Se evidenció que la entidad cuenta con un Plan Estratégico de Seguridad y Privacidad de la Información (PESI) 2024 2027, en el cual se estructuran veinte (20) proyectos asociados al MSPI. De estos, once (11) se encuentran en ejecución, seis (6) pendientes y tres (3) planificados para el año 2027.

No obstante, se identificaron inconsistencias entre el PESI, el PSPI y los cronogramas de implementación, particularmente en proyectos críticos asociados a:

- Gestión de vulnerabilidades
- Implementación de Gestión de Eventos de Seguridad SIEM

- Implementación de Detección de Respuesta Extendida XDR
- Inteligencia de amenazas
- Preparación de las TIC para la continuidad del negocio (servicio)

El aplazamiento de la implementación de estos controles hasta la vigencia 2027 representa un riesgo para la capacidad de detección, respuesta y resiliencia digital de la entidad, considerando la criticidad de los activos de información y los servicios misionales soportados por TI.

En materia normativa, se observó que:

- La Política de Seguridad de la Información vigente corresponde a la Resolución 1944 de 2016, sin evidencia de actualización formal conforme al MSPI ni a ISO 27001:2022.
- Los documentos publicados en el portal institucional aún referencian controles de la ISO 27001:2013, lo cual no es consistente con el marco normativo actualmente aplicable.

Observación 1. Desactualización del marco normativo institucional de Seguridad y Privacidad de la Información frente a la norma ISO 27001:2022

Al revisar los documentos publicados en el portal web de la entidad, en la sección de Políticas y lineamientos sectoriales e institucionales de la OTIC, se observó que algunas políticas y lineamientos de SPI se encuentran fundamentados en la norma ISO 27001:2013 y no han sido actualizados conforme a la versión vigente ISO 27001:2022, la cual es el referente técnico adoptado por el MSPI.

Los documentos identificados en esta condición son:

- Política de Seguridad de la Información para relaciones con proveedores
- Política general de gestión de seguridad de la información
- Políticas de seguridad y privacidad de la información
- Política de uso de dispositivos móviles en las redes institucionales (2022)
- Política de uso y manejo del correo electrónico institucional (2022)
- Lineamientos para el uso de la infraestructura tecnológica SED (febrero de 2022)
- Política de privacidad y condiciones de uso de portales web (marzo de 2022)

Esta situación evidencia que el marco normativo interno no se encuentra plenamente alineado con la estructura, enfoque basado en riesgos, dominios y controles definidos en ISO 27001:2022, lo cual afecta la correcta implementación y madurez del MSPI. Ver recomendación 1.

Respuesta de la Oficina de Tecnologías de la Información y las Comunicaciones

La OTIC, a través de memorando interno No I-2026-65755 de fecha 25 de mayo de 2026, contestó el Informe Preliminar respecto de la observación No 1 así: "*Una vez revisado los lineamientos y políticas cargados en la ruta https://educacionbogota.edu.co/portal_institucional/node/9714 se evidencia y acepta la observación, en ese sentido, la OTIC se compromete con establecer un plan de trabajo para realizar la actualización de estas políticas y lineamientos antes de finalizar el segundo semestre del 2026.*"

Análisis y conclusiones OCI

De acuerdo con lo aceptado por el proceso auditado, la observación se mantiene.

2.2.3. Fase de operación

Durante la auditoría, la OTIC demostró la existencia de controles técnicos y operativos, tales como:

- Herramientas de monitoreo de disponibilidad (WhatsUp Gold)
- Gestión de eventos de seguridad (FortiAnalyzer)
- Infraestructura de seguridad perimetral
- Inventario de activos de información y matriz de riesgos

Sin embargo, a partir de la revisión detallada se evidenció que:

- La Declaración de Aplicabilidad (SoA) fue aportada identificando 93 controles que son aplicables, es decir, cumple plenamente con la cobertura requerida por la norma.
- En la matriz de riesgos de seguridad de la información y seguridad digital 2025, disponible como última versión en ISOLUCION, no se evidenció la incorporación explícita de varios controles nuevos de ISO 27001:2022, tales como inteligencia de amenazas, seguridad en la nube, preparación para la continuidad del negocio, gestión de configuración, eliminación y protección avanzada de la información.
- La información relacionada con incidentes de seguridad y planes de tratamiento se presenta de forma agregada (número de solicitudes), pero sin el detalle necesario que permita evaluar la efectividad de la gestión de incidentes y vulnerabilidades.

Observación 2. Ausencia de controles de la ISO 27001:2022 en la matriz de riesgos de seguridad de la información y seguridad digital

Al revisar en el aplicativo ISOLUCION la “Matriz de riesgos de seguridad de la información y seguridad digital 2025”, y a partir de la selección de una muestra de los 11 controles que fueron incluidos en la norma ISO 27001:2022, no se evidenció información asociada a nueve de ellos que corresponden a:

- A.5.7: Inteligencia sobre amenazas
- A.5.23: Seguridad de la información para el uso de servicios en la nube
- A.5.30: Preparación de las TIC para la continuidad del negocio
- A.7.4: Monitoreo de la seguridad física
- A.8.9: Gestión de configuración
- A.8.10: Eliminación de información
- A.8.11: Enmascaramiento de datos
- A.8.23: Filtrado web
- A.8.28: Codificación segura

No se evidenció revisión e incorporación de dichos controles en la matriz, así como la actualización conforme a los lineamientos de la norma vigente lo cual afecta la implementación adecuada del MSPI. Ver recomendación 1.

Respuesta de la Oficina de Tecnologías de la Información y las Comunicaciones

La OTIC, a través de memorando interno No I-2026-65755 de fecha 25 de mayo de 2026, contestó el Informe Preliminar respecto de la observación No 2 así: "*Respecto a la observación relacionada con la presunta ausencia de controles de la ISO/IEC 27001:2022 dentro de la matriz de riesgos 2025, la OTIC, se permite presentar las siguientes consideraciones técnicas y metodológicas al respecto:*

1. La matriz de riesgos contiene información y componentes de gestión configurados en pestañas ocultas utilizadas para el tratamiento y administración de riesgos. Dentro de estas se encuentra la pestaña denominada "Matriz de Controles", la cual hace parte integral del modelo de gestión implementado por la entidad.

2. Para visualizar dicha información, la pestaña debe ser habilitada y posteriormente desbloqueada, para ello emplear la contraseña Cs1rt2023, dado que el archivo cuenta con mecanismos de protección para preservar la*
integridad de la información. Una vez realizado este procedimiento, se evidencia que la matriz trabaja con base en los 93 controles definidos por la ISO/IEC 27001:2022, incluyendo los controles relacionados en la observación,
tales como:

- *A.5.7 – Inteligencia sobre amenazas*
- *A.5.23 – Seguridad de la información para el uso de servicios en la nube*
- *A.5.30 – Preparación de las TIC para la continuidad del negocio*
- *A.7.4 – Monitoreo de la seguridad física*
- *A.8.9 – Gestión de configuración*
- *A.8.10 – Eliminación de información*
- *A.8.11 – Enmascaramiento de datos*
- *A.8.23 – Filtrado web*
- *A.8.28 – Codificación segura.*

3. Adicionalmente, es importante precisar que la Declaración de Aplicabilidad (SoA) establece los controles que la entidad considera aplicables dentro del alcance del Sistema de Gestión de Seguridad de la Información; sin embargo, ello no implica que todos los controles deban implementarse de manera simultánea o indiscriminada en cada ejercicio de gestión de riesgos.

4. Conforme a la metodología de gestión de riesgos adoptada por la entidad y alineada con los lineamientos del Departamento Administrativo de la Función Pública – DAFP, los controles son definidos e implementados a partir del análisis de contexto, valoración de activos críticos, identificación de amenazas, vulnerabilidades, evaluación del riesgo y definición del tratamiento correspondiente. En este sentido, la implementación de controles responde a
criterios de necesidad, pertinencia, proporcionalidad y eficacia frente a los riesgos identificados.

5. Bajo este enfoque metodológico, la aplicación indiscriminada de todos los controles de la ISO/IEC 27001:2022 sobre todos los activos y escenarios evaluados no solo desnaturaliza el proceso de tratamiento de riesgos, sino que afecta la eficiencia y efectividad del modelo de gestión, dado que los controles deben responder directamente a riesgos identificados y no a una implementación generalizada sin análisis previo.

Por lo anterior, se considera que la matriz de riesgos sí contempla y gestiona los controles definidos en la ISO/IEC 27001:2022 conforme al alcance, criticidad y resultados del proceso de gestión de riesgos implementado por la entidad."

Análisis y conclusión OCI

Conforme a la respuesta emitida por la OTIC donde manifiesta que existe una *"Matriz de Controles"* en la que se contempla y gestiona los controles de los riesgos mencionados. Luego de la nueva validación realizada por la OCI a la Matriz de Riesgos 2025 publicada en el aplicativo ISOLUCION, no se evidencia el registro de los riesgos señalados, y adicionalmente la OCI considera que no es coherente la implementación de controles sobre riesgos que no están previamente identificados, lo cual no corresponde a la metodología para la gestión integral de riesgos de la SED. Por lo anterior la observación de mantiene.

2.2.4. Fase de evaluación del desempeño

La auditoría evidenció que los indicadores de gestión del MSPI se encuentran en etapa de formulación, contando con fichas técnicas preliminares para cuatro (4) indicadores; sin embargo:

- No se encuentran aprobados formalmente
- No se ha definido línea base
- No se han realizado mediciones ni análisis de desempeño

En consecuencia, la entidad no cuenta aún con mecanismos consolidados de medición que permitan evaluar objetivamente la madurez y efectividad del MSPI.

2.2.5. Fase de mejora continua

La OTIC reportó la existencia de matrices de acciones correctivas y de mejora derivadas del análisis de Brechas GAP, autodiagnóstico y SoA. No obstante, la evidencia aportada no permitió verificar integralmente la trazabilidad entre hallazgos, causas, acciones, responsables y cierre efectivo, por lo que, si bien el enfoque de mejora continua está definido, su aplicación es poco perceptible.

2.2.6. Conclusión del estado de implementación del MSPI

De acuerdo con la evidencia revisada, el MSPI en la SED se encuentra implementado de manera parcial, con avances en estructuración, planeación y algunos controles operativos, pero con debilidades en documentación actualizada, formalización de controles ISO 27001:2022, medición del desempeño y cierre efectivo del ciclo de mejora continua. Estas condiciones limitan la capacidad del MSPI para operar como un habilitador integral de la Política de Gobierno Digital y de la gestión de riesgos de seguridad digital de la entidad.

2.3. Avance en la implementación de los controles nuevos de la ISO 27001:2022

La Secretaría de Educación del Distrito presenta un alto nivel de avance en la implementación del conjunto de controles de la norma ISO 27001:2022, evidenciándose que los 93 controles aplicables han sido incorporados en el marco del SGSI, con predominio de estados "Gestionado" y "Optimizado", y con una meta institucional definida de alcanzar el 100 % en nivel optimizado para

el año 2027.

No obstante, la auditoría identificó debilidades específicas principalmente asociadas a:

- Desactualización de políticas y lineamientos frente a la versión vigente de la norma.
- Ausencia de formalización en los controles nuevos introducidos por ISO 27001:2022.

Observación 3 - Desactualización normativa frente a ISO 27001:2022

Durante la revisión en la matriz SoA de 40 controles, equivalentes al 43% de la población (93), en la que se incluyen los controles A.5.1, A.5.2, A.5.10, A.5.11, A.7.7, A.7.9, A.7.14 y A.8.10, se evidenció que los Lineamientos de la Política de Seguridad y Privacidad de la Información SED (versión 2020) y el Manual de la Política del SGSI continúan referenciando a la norma ISO 27001:2013 y a la guía ISO 27002:2013, pese a que la entidad se encuentra en proceso de implementación de la versión ISO 27001:2022. Lo descrito, incumple la Resolución MinTIC 500 de 2021, actualizada por la Resolución 02277 de 2025; ISO 27001:2022, cláusulas 5 y 7.5 (información documentada); MSPI – principio de actualización y coherencia normativa. El mantenimiento y actualización de los instrumentos normativos del SGSI no se ha realizado de forma oportuna ni sincronizada con la adopción de la nueva versión de la norma ISO 27001:2022. Adicionalmente, los controles A.5.30, A.8.9, A.8.12 y A.8.16 de la norma ISO 27001:2022 tienen como evidencia procedimientos aprobados mediante la Resolución 5 del 24 de diciembre de 2021. La desactualización normativa puede generar inconsistencias en la aplicación, evaluación y auditoría del SGSI, así como interpretaciones erróneas sobre los controles vigentes, afectando la coherencia del sistema y la trazabilidad del cumplimiento frente a estándares actualizados. Ver recomendación 3.

Respuesta de la Oficina de Tecnologías de la Información y las Comunicaciones

La OTIC, a través de memorando interno No I-2026-65755 de fecha 25 de mayo de 2026, contestó el Informe Preliminar respecto de la observación No 3 así: "*En atención a la Observación 3, formulada en el marco de la auditoría al Sistema de Gestión de Seguridad de la Información (SGSI) de la Secretaría de Educación del Distrito y, relacionada con la referenciación de la norma ISO 27001:2013 en los instrumentos normativos vigentes, la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC), a través del Grupo CSIRT, informa lo siguiente:*

La OTIC adelanta actualmente el proceso de actualización de los Lineamientos de la Política de Seguridad y Privacidad de la Información y del Manual del SGSI, para referenciar de manera expresa la versión ISO 27001:2022 e ISO 27002:2022, en relación con la Resolución MinTIC 02277 de 2025 y el principio de actualización y coherencia normativa del MSPI.

Por lo anterior, la OTIC informa que el SGSI se encuentra operativamente activo y que los controles de seguridad asociados a los controles observados se aplican de manera continua y documentada. Como evidencia, se adjunta al presente oficio el Informe de Gestión de Seguridad de la Información — SED, correspondiente al periodo auditado desde el 1 de enero de 2025, en el cual se documentan las actividades de monitoreo de amenazas, gestión de vulnerabilidades técnicas, atención de solicitudes e incidentes de seguridad, y operación de la infraestructura de seguridad perimetral (IDS, IPS, Fortinet), evidenciando la aplicación efectiva de los controles A.5.1, A.5.2, A.5.10, A.5.11, A.7.7, A.7.9, A.7.14, A.8.9, A.8.10, A.8.12, A.8.16 y A.5.30 de la norma ISO

27001:2022."

Análisis y conclusión OCI

De acuerdo con la respuesta de la OTIC en la que afirma: "*La OTIC adelanta actualmente el proceso de actualización de los Lineamientos de la Política de Seguridad y Privacidad de la Información y del Manual del SGSI, para referenciar de manera expresa la versión ISO 27001:2022 … y el principio de actualización y coherencia normativa del MSPI", se* confirma que se requiere fortalecer la actualización normativa y la formalización documental y por tanto la observación se mantiene.

2.4. Seguimiento al reporte anual del FURAG 2024 (Gobierno Digital y Seguridad Digital)

Se realizó validación técnica y documental de 87 preguntas del Formulario Único de Reporte de Avance a la Gestión (FURAG) 2024, específicamente en lo relacionado a Gobierno Digital y Seguridad Digital. En esta evaluación se pretendió hacer un diagnóstico de la madurez de las capacidades institucionales frente a los requisitos de la Resolución MinTIC 500/2021, actualizada por la Resolución 02277 de 2025, y los controles de resiliencia de la norma ISO 27001:2022.

Tras la revisión de las preguntas con número SED200 a SED203, se confirmó que la entidad ha fortalecido su metodología para identificar, gestionar y mitigar riesgos de seguridad digital. La coherencia detectada entre el reporte y la Matriz de Riesgos de Seguridad Digital evidencia un proceso de tratamiento activo alineado con el MSPI, donde se priorizan los activos críticos de información. No obstante, se resalta la necesidad de evolucionar estos análisis hacia modelos de evaluación de impacto cuantitativo que reflejen la dinámica de las nuevas amenazas identificadas en la Resolución 02277 de 2025. En cuanto al bloque SED213 a SED232, se enfatiza la solidez en la gestión de copias de respaldo (SED215) y la operatividad de protocolos de autenticación avanzada como DMARC, DKIM y SPF (SED232), los cuales son controles críticos para garantizar la integridad y disponibilidad de la información según los estándares de la ISO 27001:2022.

Con relación al Gobierno Digital, se verificó un cumplimiento sobresaliente en la formalización de la Política de Seguridad y Privacidad de la Información (GDI233), la cual se encuentra alineada con el marco normativo vigente y debidamente socializada a través de los canales institucionales.

Si bien los procesos de gestión de vulnerabilidades (SED231) y parches (SED213) son positivos, la auditoría identificó que existe oportunidad de establecer un sistema de escaneos periódicos que incluya monitoreo continuo y pruebas de intrusión proactivas (Ethical Hacking) para validar la efectividad de los controles de mitigación en entornos de infraestructura crítica. Ver Recomendación 4.

En cuanto a la formulación de Planes de Mejoramiento asociados a las recomendaciones del Departamento Administrativo de la Función Pública DAFP, se confirma que el 100% de las preguntas evaluadas cuentan con acciones de seguimiento integradas en el Plan de Trabajo OTIC 2025. Esta integración garantiza que las recomendaciones emitidas por el DAFP se traduzcan en compromisos institucionales con responsables y fechas de cumplimiento definidas.

Finalmente, y en base a las pruebas de auditoría realizadas, se concluye que el componente de autodiagnóstico FURAG 2024 de la SED muestra una capacidad institucional tolerable para el

tratamiento de riesgos de seguridad digital. De igual forma, la entidad posee una estructura de gobernanza robusta y controles técnicos operativos que proporcionan una seguridad razonable sobre el cumplimiento de la Resolución MinTIC 500/2021 y su actualización de 2025, lo anterior sienta bases firmes para una implementación más robusta bajo el estándar ISO 27001:2022.

2.5. Seguimiento a los planes de mejoramiento resultado de la Auditoria Gobierno y Seguridad Digital - Quejas servicio de conectividad en Colegios - PAA 2025.

En el marco de la presente auditoría, se realizó la evaluación de los Planes de Mejoramiento (PM) formulados como respuesta a las observaciones 1897, 1900, 1901 y 1902, generadas durante la auditoría Gobierno y Seguridad Digital 2025.

La evaluación de los PM tuvo como propósito verificar el grado de avance, cumplimiento y efectividad de las acciones definidas, así como la existencia de evidencias que respalden su ejecución y contribuyan a la mitigación de los riesgos asociados a la seguridad digital. Para tal efecto, se analizó la coherencia entre los hallazgos identificados, las acciones formuladas, los responsables asignados, los plazos establecidos y los mecanismos de seguimiento implementados.

2.5.1. Observación 1897.

En relación con la observación asociada al monitoreo y control de riesgos en la supervisión de contratos a cargo de la OTIC, se evidenció la implementación efectiva de las acciones definidas en el PM.

La dependencia acreditó el monitoreo periódico de los riesgos contractuales mediante la inclusión sistemática del capítulo de riesgos en los informes mensuales de ejecución de los contratos, dando cumplimiento a lo establecido en el Artículo 10 del Manual de Supervisión de la SED. Dichos informes permiten identificar, evaluar y realizar seguimiento a los riesgos asociados a los contratos supervisados, así como definir acciones para su tratamiento oportuno. Por tanto, las evidencias aportadas resultaron suficientes, pertinentes y verificables, y demuestran que el monitoreo y control de riesgos se integró de manera formal y continua al proceso de supervisión contractual, contribuyendo a la mitigación de riesgos operativos, financieros y reputacionales, relevantes también desde el enfoque de seguridad digital.

En consecuencia, se concluye que el PM asociado al hallazgo cumplió plenamente con su objetivo, por lo cual el resultado de la evaluación es Cumple (100) y se procede al cierre del hallazgo.

2.5.2. Observación 1900.

En relación con la observación asociada a la ausencia de evidencia de ejecución de controles definidos en diversos procedimientos del proceso de Gobierno y Seguridad Digital, se evaluó el avance del PM formulado por la dependencia responsable.

Como resultado de las acciones reportadas, se evidenció que el PM se encuentra registrado y presenta avances parciales, en tanto se expidió Resolución 004 de 2025 para la actualización de dos (2) procedimientos, específicamente el 12-PD-027 “Mantenimiento de Soluciones Informáticas” y el 12-MN-004 “Lineamientos de Protección de Registros”, lo cual constituye un avance frente a la

situación inicialmente identificada.

No obstante, la cobertura y ejecución integral de la acción presenta debilidades, dado que los procedimientos restantes señalados en el hallazgo no cuentan aún con evidencia de actualización formal ni con soporte que permita verificar la validación de los controles definidos. Así mismo, no se evidenció un plan de seguimiento o monitoreo que permita asegurar que las actualizaciones realizadas responden de manera efectiva a los controles requeridos ni que se garantice su aplicación sistemática en los demás procedimientos pendientes.

En consecuencia, aunque se reconocen avances iniciales en la atención del hallazgo, estos no resultan suficientes para dar cumplimiento total a la acción formulada ni para mitigar de manera integral el riesgo identificado, motivo por el cual el resultado de la evaluación del PM es Parcialmente cumple (50) y el hallazgo permanece abierto, a la espera de la ejecución completa de las acciones y del seguimiento correspondiente.

2.5.3. Observación 1901.

Con relación a la observación relacionada con el incumplimiento parcial de los controles definidos en el Anexo A de la norma ISO/IEC 27001:2013 por parte del Proceso de Gobierno y Seguridad Digital, se evaluó la efectividad del PM formulado para atender las debilidades identificadas.

Como resultado de la revisión realizada, se evidencian avances significativos en la planeación, estructuración e implementación progresiva de los controles de seguridad de la información, reflejados en la formalización del plan de trabajo, la aprobación por parte de la alta dirección, la elaboración del Statement of Applicability (SoA) versión 2022 y el fortalecimiento de varios controles considerados críticos dentro del SGSI.

Sin embargo, la evidencia aportada también permite establecer que persisten controles en estado parcial o no implementado, cuyo cumplimiento fue proyectado para vigencias futuras, en atención al proceso de transición normativa, considerando que la versión ISO 27001:2013 mantiene vigencia hasta octubre de 2025. Esta situación no permite confirmar, a la fecha de la auditoría, la efectividad operativa completa de todos los controles, ni la mitigación total del riesgo identificado, especialmente en dominios críticos como la seguridad física y del entorno, así como la adquisición, desarrollo y mantenimiento de sistemas de información. De igual forma, no hay evidencia suficiente, pertinente y verificable que demuestre la ejecución de los controles indicados en el desarrollo documental.

En consecuencia, aunque se reconocen avances relevantes y consistentes en la implementación del SGSI, estos no resultan suficientes para acreditar el cumplimiento integral del Anexo A ni para proceder al cierre del hallazgo. Por lo anterior, el resultado de la evaluación del PM es Parcialmente cumple (50) y el hallazgo permanece abierto, sujeto a la implementación completa y verificación de la efectividad de los controles pendientes.

2.5.4. Observación o hallazgo 1902.

Con relación a la observación asociada al incumplimiento de controles definidos en la Matriz de Seguridad de la Información de la SED, se evaluó el avance y efectividad del PM formulado por la OTIC.

Como resultado del proceso de seguimiento, se evidencian avances relevantes en la formalización normativa y en la estructuración de evidencias relacionadas con los controles observados, en particular aquellos asociados al manejo de activos, seguridad física y del entorno, copias de seguridad, requisitos de seguridad de los sistemas de información y disponibilidad de las instalaciones de procesamiento de información. Dichos avances reflejan esfuerzos orientados a fortalecer el SGSI, en concordancia con los lineamientos de la Política de Seguridad y Privacidad de la Información de la SED y los estándares ISO/IEC 27001 y 27002.

No obstante, la información aportada no permite verificar de manera completa el seguimiento, monitoreo y evaluación sistemática de los controles establecidos en la Matriz de Seguridad de la Información, evidenciándose brechas en la demostración de su efectividad operativa. En particular, persisten debilidades para acreditar que los controles implementados se ejecutan de forma periódica, consistente y verificable, más allá de su formalización documental, lo cual limita la confirmación de la mitigación integral del riesgo identificado.

En consecuencia, si bien se reconocen avances parciales en la atención del hallazgo, estos no resultan suficientes para demostrar el cumplimiento pleno de los controles definidos ni para proceder al cierre de este. Por lo anterior, el resultado de la evaluación del PM es Parcialmente cumple (50) y el hallazgo permanece abierto, a la espera de evidencias adicionales que acrediten la aplicación efectiva, el seguimiento y la evaluación continua de los controles establecidos. Ver Recomendación 5.

2.6. Resultados de las pruebas de recorrido a la infraestructura (Data Center)

Con el fin de verificar la implementación de los controles físicos definidos en la norma ISO 27001:2022, se realizaron pruebas de recorrido a los centros de datos CTD CLL 17, CDI CLL 63 y NVC CLL 26, evaluando los controles del dominio A.7 “Controles físicos”.

Las pruebas de recorrido evidenciaron que la entidad cuenta con controles físicos implementados y operativos en los centros de datos visitados; sin embargo, se identificaron debilidades recurrentes en varios controles críticos, los cuales fueron calificados como “Parcialmente” cumplidos de manera sistemática en las tres sedes, configurando incumplimientos frente a los requisitos de la ISO 27001:2022.

El no contar con protección perimetral suficiente, incrementa el riesgo de accesos no autorizados, sabotaje, daño intencional o interrupción de la operación, lo cual puede afectar la disponibilidad e integridad de los servicios tecnológicos misionales de la entidad, interrupciones no controladas de los servicios tecnológicos, pérdida de información o afectación de activos críticos, impactando la continuidad operativa.

En este mismo contexto, se evidenció en las pruebas de recorrido y entrevistas realizadas, deficiencias en las instalaciones del CDI - Calle 63, denominado como “Datacenter Principal”, es decir, las instalaciones y controles implementados, no cumplen con los requerimientos, mejores prácticas y estándares requeridos para este tipo de Datacenter (ANSI/TIA/EIA-942 parámetros mecánicos, eléctricos, arquitectónicos y de comunicación para la mejor ejecución de los data center).

Adicionalmente, se identificaron fallas y deficiencias significativas en los sistemas de control de temperatura, refrigeración, incendios e iluminación de emergencia; con el riesgo de adecuaciones

sin el lleno de los requisitos requeridos en un Datacenter, como instalación de ductos de refrigeración para llevar el aire hasta la totalidad de los equipos de misión crítica, principales o core, es decir, donde se alojan las aplicaciones y servicios esenciales de la SED.

Al ingresar a estas instalaciones se observó, en general, que las mismas no corresponden a un "Datacenter Principal", en razón a que la temperatura es alta y constante, algunos equipos presentan obsolescencia tecnológica y fuera de servicio de soporte y mantenimiento, y otros no están debidamente identificados ni protegidos, ejemplo contra accesos no autorizado a personal de los proveedores de telecomunicaciones y servicios TIC, entre otros.

La planificación de la seguridad física en los Datacenter, centros de datos, cableado y de procesamiento de información de la SED, no ha incorporado de manera integral el análisis del contexto externo y del entorno de amenazas, limitando la adopción de controles diferenciados, según la ubicación y exposición de dichos centros de datos.

Observación 4 – Insuficiencia en la protección del perímetro físico de los centros de datos frente a amenazas físicas y ambientales

Durante la visita a los centros de datos CTD-CLL17, CDI-CLL63 y NVC-CLL 26, se evidenció que, si bien existe seguridad física perimetral básica, no se han implementado controles suficientes para mitigar riesgos mitigar riesgos y amenazas físicas y ambientales asociados a vandalismo, asonadas, terrorismo e inseguridad del entorno ni cubren de forma integral todos los riesgos originados en eventos ambientales. El control A.7.1 fue calificado como "Parcialmente" cumplido con relación a la ISO 27001:2022, de igual forma se evaluaron los controles A.7.1 Perímetros de seguridad física control, A.7.5 Protección contra amenazas físicas y ambientales. ISO 27002:2022 – Directrices sobre protección perimetral reforzada en zonas de riesgo. La planificación de la seguridad física no ha incorporado de manera integral el análisis del contexto externo y del entorno de amenazas, limitando la adopción de controles diferenciados según la ubicación y exposición de los centros de datos. La insuficiente protección perimetral incrementa el riesgo de accesos no autorizados, sabotaje, daño intencional o interrupción de la operación, lo cual puede afectar la disponibilidad e integridad de los servicios tecnológicos misionales de la entidad, interrupciones no controladas de los servicios tecnológicos, pérdida de información o afectación de activos críticos, impactando la continuidad operativa. Ver recomendación 6.

Respuesta de la Oficina de Tecnologías de la Información y las Comunicaciones

La OTIC, a través de memorando interno No I-2026-65755 de fecha 25 de mayo de 2026, contestó el Informe Preliminar respecto de la observación No 4 así: *"Respecto a la observación relacionada con la insuficiencia en la protección del perímetro físico de los centros de datos frente a amenazas físicas y ambientales, es importante precisar que los controles evaluados corresponden a componentes con responsabilidades compartidas entre diferentes áreas de la entidad.*

En relación con el control A.7.1 – Perímetros de seguridad física, se informa que la administración, operación y fortalecimiento de los controles de seguridad física perimetral de las sedes institucionales no se encuentra bajo la competencia directa de la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC, sino del área encargada de Servicios Administrativos y de los contratos asociados a vigilancia y seguridad física de la entidad. En este sentido, los componentes relacionados con control perimetral físico, vigilancia, control de acceso externo, protección de instalaciones y demás medidas de seguridad física del entorno son gestionados

desde dicha dependencia conforme a sus competencias funcionales y contractuales.

No obstante, la OTIC ha venido adelantando acciones de fortalecimiento gradual de la infraestructura de Data Center, en función de las capacidades presupuestales, restricciones de infraestructura física existente y priorización institucional de riesgos tecnológicos, teniendo en cuenta además que parte de los servicios misionales y plataformas estratégicas de la entidad operan actualmente bajo esquemas híbridos que integran infraestructura on premise y servicios en nube Microsoft Azure y Oracle OCI, contribuyendo a mejorar los niveles de resiliencia tecnológica y continuidad operativa institucional.

Frente al control A.7.5 – Protección contra amenazas físicas y ambientales, la OTIC adelantó durante la vigencia 2025 gestiones orientadas a la identificación y evaluación de riesgos ambientales sobre los centros de datos institucionales. Como evidencia de ello, se radicó ante el Instituto Distrital de Gestión de Riesgos y Cambio Climático – IDIGER la solicitud No. 20250995, mediante la cual se requirió apoyo técnico para la evaluación de riesgos derivados de amenazas físicas y medioambientales, incluyendo incendios, inundaciones, terremotos, explosiones, disturbios civiles, residuos tóxicos, emisiones medioambientales y demás eventos naturales o antrópicos que pudieran afectar los sitios CDI Centro de Innovación, NVC Nivel Central y CTD Centro de Transformación Digital.

No obstante, el IDIGER informó que parte del alcance requerido no correspondía a sus competencias técnicas y funcionales, razón por la cual no fue posible obtener una evaluación integral sobre todos los escenarios de riesgo solicitados.

En consecuencia, la OTIC reconoce que el control actualmente presenta un estado de implementación parcial, situación que ya había sido identificada dentro del proceso de evaluación del Sistema de Gestión de Seguridad de la Información, por ello el radicado ante el IDIGER. Así mismo, es importante precisar que la implementación integral de este tipo de controles requiere articulación interinstitucional, acompañamiento técnico especializado y participación de múltiples dependencias responsables de infraestructura física, continuidad, seguridad física y gestión del riesgo. En este sentido, la OTIC continuará adelantando las gestiones necesarias para fortalecer el análisis de amenazas físicas y ambientales sobre la infraestructura tecnológica crítica de la entidad, conforme a las capacidades institucionales y competencias definidas para cada área involucrada.

Análisis y conclusión OCI

En su respuesta la OTIC ratifica que: "*el control actualmente presenta un estado de implementación parcial… la OTIC continuará adelantando las gestiones necesarias para fortalecer el análisis de amenazas físicas y ambientales sobre la infraestructura tecnológica crítica de la entidad".* Por lo anterior se confirma la observación.

Observación 5 – Deficiencias en la gestión integral de activos físicos y medios de almacenamiento

En el centro de datos CDI-CLL63 y NVC-CLL26 se evidenció cumplimiento parcial en los controles:

- A.7.8 Ubicación y protección del equipo
- A.7.10 Medios de almacenamiento

- A.7.12 Seguridad del cableado
- A.7.13 Mantenimiento de equipos
- A.7.14 Eliminación segura o reutilización de equipos

Lo anterior incumple lo establecido en la ISO 27001:2022 – Controles A.7.8, A.7.10, A.7.12, A.7.13 y A.7.14. La gestión de infraestructura física se encuentra distribuida entre diferentes responsables, sin lograr adecuados controles físicos en todas las sedes.

Si bien la entidad ha implementado controles físicos básicos en sus centros de datos, los resultados de las pruebas de recorrido evidencian que la infraestructura tecnológica crítica no cuenta aún con un nivel de protección integral y homogéneo, de acuerdo con los requerimientos de la ISO 27001:2022. Ver recomendación 7.

Estas deficiencias incrementan el riesgo de daño físico, pérdida de información, filtración de datos o fallas operativas, afectando la confidencialidad, integridad y disponibilidad de la información institucional.

Respuesta de la Oficina de Tecnologías de la Información y las Comunicaciones

La OTIC, a través de memorando interno No I-2026-65755 de fecha 25 de mayo de 2026, contestó el Informe Preliminar respecto de la observación No. 5 así: *"Respecto a la observación relacionada con presuntas deficiencias en la gestión integral de activos físicos y medios de almacenamiento, se presentan las siguientes precisiones frente a los controles evaluados:*

La administración de la infraestructura tecnológica de la SED se soporta en contratos especializados de operación, soporte y mantenimiento de Data Center, mesa de servicios e infraestructura TIC, mediante los cuales se ejecutan actividades periódicas de monitoreo, soporte técnico, mantenimiento y acompañamiento operativo sobre los componentes críticos de la plataforma tecnológica institucional.

Frente al control A.7.8 – Emplazamiento y protección de equipos, no resulta procedente acoger la observación, toda vez que, la entidad sí cuenta con lineamientos y controles implementados para la ubicación, acceso y protección de equipos críticos de infraestructura tecnológica, evidenciados en la política interna de acceso a Data Center y cuartos de comunicaciones administrada por la OTIC. Dicho documento establece controles relacionados con acceso autorizado, restricciones físicas, medidas de protección sobre infraestructura tecnológica crítica, control de visitantes, acompañamiento, monitoreo y condiciones de seguridad para el acceso a áreas sensibles, alineándose con lo establecido por la ISO/IEC 27001:2022 esta política se encuentra en la URL compartida Controles ISO 27001 donde se encuentra el control A7.8.

Por otra parte, se hace claridad que esta política no se encuentra publicada en ISOLUCIÓN ni en el portal institucional debido a que corresponde a un documento interno de seguridad de la OTIC con acceso restringido por su naturaleza técnica y operativa.

Respecto a los controles:
• A.7.10 – Medios de almacenamiento
• A.7.12 – Seguridad del cableado
• A.7.13 – Mantenimiento de equipos
• A.7.14 – Eliminación segura o reutilización de equipos

Es importante acarar que estos controles hacen parte del plan interno de implementación y fortalecimiento del Sistema de Gestión de Seguridad de la Información aprobado por la Jefatura de la OTIC, encontrándose actualmente en fases de elaboración, adopción e implementación progresiva conforme a la planeación institucional definida. Las fechas proyectadas de implementación son:
• A.7.10 – 27/12/2027
• A.7.12 – 30/03/2028
• A.7.13 – 15/04/2028
• A.7.14 – 15/04/2026

Es importante precisar que la adopción de controles asociados a la actualización de la ISO/IEC 27001:2022 dentro de entidades públicas corresponde a un proceso progresivo de madurez y adecuación institucional, alineado con el Modelo de Seguridad y Privacidad de la Información – MSPI y con los lineamientos de Gobierno Digital definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC. El MinTIC, mediante la actualización del MSPI efectuada a través de la Resolución 2277 de 2025, indicó que la incorporación de la ISO/IEC 27001:2022 corresponde a un proceso de fortalecimiento gradual de las capacidades de seguridad digital de las entidades públicas, bajo esquemas de gestión del riesgo, mejora continua y adecuación progresiva de controles, metodologías y lineamientos institucionales.

Así mismo, el Modelo de Seguridad y Privacidad de la Información – MSPI establece que la implementación de controles debe desarrollarse mediante procesos de planeación, implementación, evaluación y mejora continua, alineados con el contexto organizacional, la criticidad de los activos, la capacidad operativa y la gestión de riesgos de cada entidad.

En este sentido, la implementación de controles no corresponde a una adopción inmediata y simultánea de la totalidad de controles definidos por la ISO/IEC 27001:2022, sino a un proceso planificado y priorizado conforme al análisis de riesgos, el nivel de madurez institucional, la disponibilidad presupuestal y las capacidades técnicas y operativas de la entidad.

Adicionalmente, la ISO/IEC 27001:2022 se fundamenta en un modelo basado en riesgos y mejora continua, donde los controles deben implementarse de manera proporcional y pertinente frente a los riesgos identificados, evitando implementaciones indiscriminadas que puedan afectar la eficiencia y efectividad del Sistema de Gestión de Seguridad de la Información.

Por lo anterior, se evidencia que la OTIC ha venido adelantando acciones de implementación, fortalecimiento y planificación sobre los controles observados, conforme con los lineamientos técnicos y metodológicos aplicables al sector público.

Como elemento complementario a las acciones de fortalecimiento descritas, la OTIC considera importante resaltar que la entidad adelanta actualmente el proyecto de traslado de la sede central NVC CLL 26 hacia una nueva ubicación institucional, escenario que representa una oportunidad estratégica para incorporar mejoras integrales en materia de infraestructura tecnológica, seguridad física y continuidad operativa. En el marco de dicho proceso se prevé fortalecer aspectos relacionados con el diseño y organización del cableado estructurado, adecuación de espacios técnicos especializados para centros de distribución de cableado y optimización de las condiciones físicas y ambientales del centro de comunicaciones, fortalecimiento de controles de acceso físico, monitoreo y seguridad, así como reforzamiento de mejores prácticas alineadas con ISO

27001:2022, MSPI y estándares aplicables para infraestructura tecnológica crítica. Estas acciones contribuirán a mitigar riesgos identificados durante las pruebas de recorrido realizadas por el equipo auditor, incrementando los niveles de disponibilidad, resiliencia, protección y continuidad de los servicios tecnológicos misionales de la entidad.

Referencias de soporte:

- *MSPI – MinTIC*
- *Actualización del MSPI – Resolución 2277 de 2025*
- *Resolución 500 de 2021 – Seguridad Digital y MSPI"*

Análisis y conclusión OCI

En su respuesta la OTIC informa que los controles de seguridad física se encuentran *"… actualmente en fases de elaboración, adopción e implementación progresiva…"* con fechas proyectadas de implementación 2027 y 2028, relacionando acciones de mejora con las cuales: "*se prevé fortalecer aspectos relacionados con el diseño y organización del cableado estructurado, adecuación de espacios técnicos especializados para centros de distribución de cableado y optimización de las condiciones físicas y ambientales del centro de comunicaciones, fortalecimiento de controles de acceso físico, monitoreo y seguridad, así como reforzamiento de mejores prácticas alineadas con ISO 27001:2022, MSPI y estándares aplicables para infraestructura tecnológica crítica*. *Estas acciones contribuirán a mitigar riesgos identificados durante las pruebas de recorrido realizadas por el equipo auditor, incrementando los niveles de disponibilidad, resiliencia, protección y continuidad de los servicios tecnológicos misionales de la entidad" (subrayado fuera de texto).* Teniendo en cuenta el tiempo futuro de estas acciones correctivas la observación se confirma.

De otro lado y con relación a la solicitud de unificación de las observaciones, que se entiende como una aceptación tácita de lo registrado en la auditoría, se invita al proceso a la articulación de las acciones de mejoramiento orientadas a subsanar la causa raíz de los hallazgos considerados como comunes por el proceso auditado.

2.7. Evaluación al Sistema de Control Interno - Formulario MECI

El Modelo Estándar de Control Interno – MECI es el instrumento que permite identificar el estado de implementación y madurez del sistema de control interno en una entidad, proceso o actividad. A partir de los componentes del MECI se posibilita la búsqueda de oportunidades de mejora que fortalecen la estructura de reporte y control que aseguran el cumplimiento de los objetivos institucionales y la satisfacción de las expectativas de las partes interesadas.

Por lo anterior los ejercicios de auditoría deben considerar en su alcance la evaluación del sistema de control interno SCI y desde la evidencia objetiva reconocer las acciones de los sujetos de auditoría y recomendar acciones de consolidación del sistema de control interno.

2.7.1. Ambiente De Control

Este componente permite identificar el compromiso de los niveles superiores con la implementación, monitoreo y mejora continua del sistema de control interno. Incluye actividades de fomento del código de integridad, roles y responsabilidades en la estructura de control, líneas de reporte y articulación con los objetivos estratégicos de la entidad.

En este aspecto es destacable el compromiso con el código de ética de la SED, especialmente para un aspecto tan sensible como la seguridad de la información. Igualmente, la definición y documentación de roles y responsabilidades y la rendición de informes a la alta dirección confirman la importancia institucional a la seguridad de la información que se refleja en los resultados anuales del FURAG.

2.7.2. Actividades De Control

El equipo de trabajo responsable de los lineamientos asociados a la política de seguridad de la información mantiene el monitoreo de las directrices emanadas desde el MinTIC y que son de relevancia para la seguridad de la información, procurando su actualización. En este sentido, es importante que se agilice la actualización de aquellos documentos que aún refieren normas sin vigencia y se fortalezca la socialización de las versiones vigentes en el equipo de trabajo de la política.

2.7.3. Evaluación De Riesgos

El monitoreo a los riesgos es una condición necesaria en la gestión de lo público y en ese entorno los responsables desde la OTIC otorgan prioridad al diseño de controles que contribuyan a la materialización de riesgos en el entorno de la seguridad de la información. Es recomendable fortalecer las evaluaciones de riesgos asociados a seguridad física especialmente de los puntos donde se gestionan los datos, aplicativos y equipos de alto valor para la Secretaría. Por ello la matriz de riesgos de los riesgos de seguridad de la información se monitorea de manera adecuada y se reporta de acuerdo con los lineamientos de la Oficina Asesora de Planeación.

2.7.4. Información Y Comunicación

Los canales externos e internos permiten la comunicación fluida, transparente y oportuna entre los responsables de la política de seguridad de la información y las partes interesadas, permitiendo acciones y respuestas oportunas a los cambios en el entorno, identificando la importancia de los momentos de comunicación a los 3 niveles de la SED con las recomendaciones y protocolos de seguridad a los usuarios y también con los seguimientos y reportes tanto al equipo técnico de seguridad digital como al Comité CIGD.

2.7.5. Actividades De Monitoreo

Este componente visibiliza la importancia de la autoevaluación como primer insumo para la mejora continua y en el marco de la política de seguridad de la información se observó que se establecen además de los roles y responsabilidades, las líneas de reporte y los momentos de evaluación institucional sobre el estado de riesgos y controles, oportunidades de mejora y articulación con otras políticas que se reflejan en los resultados de mediciones externas sobre la madurez de la política de seguridad de la información y la confianza institucional que genera la misma. Igualmente se evidencia un esfuerzo constante en el seguimiento a las acciones de mejora producto de auditorías internas, con oportunidades de mejora en el cumplimiento de las acciones correctivas de manera que se subsanen las debilidades identificadas dentro de los tiempos establecidos.

III. CONCLUSIONES

Como resultado de la auditoría a la Política de Seguridad y Privacidad de la Información de la Secretaría de Educación del Distrito, se concluye que la entidad cuenta con una adecuada gestión de la seguridad de la información, reflejada en una estructura de gobernanza definida, controles técnicos operativos activos y compromiso de la alta dirección con el control interno y la protección de la información.

No obstante, la auditoría evidenció que el MSPI se encuentra implementado de manera parcial, con un nivel de madurez intermedio. Si bien existen avances importantes en planeación, operación y adopción de controles de la norma ISO 27001:2022, se observaron debilidades que limitan la consolidación del modelo. En particular, se identifican brechas en la actualización del marco normativo interno, la formalización de controles nuevos incorporados por la versión 2022 de la norma y el cierre efectivo del ciclo de mejora continua.
La no actualización de lineamientos y procedimientos frente a la normativa vigente constituye un riesgo transversal, en tanto puede generar inconsistencias en la aplicación de controles y dificultades en la evaluación del cumplimiento. Esta situación se ve reforzada por la incorporación incompleta de controles en la matriz de riesgos y por la limitada trazabilidad entre hallazgos, acciones correctivas y evidencias de cierre efectivo en la gestión de los PM.

Desde la perspectiva del Sistema de Control Interno, los resultados son favorables en términos de ambiente de control, comunicación, gestión de riesgos y monitoreo, destacándose el uso del FURAG como herramienta de autodiagnóstico y mejora. Aun así, se identifican oportunidades para agilizar la actualización normativa, robustecer la gestión de riesgos físicos y fortalecer la ejecución oportuna de acciones correctivas.

Las pruebas de recorrido a los centros de datos evidencian que, aunque existen controles físicos básicos en funcionamiento, la protección de la infraestructura tecnológica crítica no es homogénea ni integral frente a los riesgos actuales del entorno físico y ambiental. Estas debilidades representan un riesgo relevante para la continuidad de los servicios tecnológicos y la disponibilidad de la información institucional, por lo que requieren atención prioritaria.

La SED se encuentra en camino hacia la consolidación de su política de seguridad digital, siendo necesario para avanzar a un nivel de madurez alto, acelerar la actualización normativa, fortalecer la formalización y seguimiento de los controles críticos, mejorar la medición del desempeño y asegurar la implementación efectiva de las acciones de mejora, de manera que el MSPI opere plenamente.

IV. RECOMENDACIONES

Recomendación 1:

Fortalecer la consolidación y actualización integral del MSPI, priorizando la formalización y armonización de los instrumentos clave del modelo, con el fin de asegurar coherencia normativa, trazabilidad y madurez del SGSI.

En particular, se recomienda:

- Consolidar y documentar de manera verificable el autodiagnóstico del MSPI y su análisis de brechas, asegurando su disponibilidad como insumo base para la planeación,

seguimiento y mejora continua.

- Actualizar y ajustar los instrumentos normativos, políticas y repositorios institucionales, alineándolos con la versión vigente de la norma ISO 27001:2022 y los lineamientos actualizados del MSPI.

- Revisar y, de ser posible, anticipar la implementación de controles estratégicos actualmente programados a mediano plazo, considerando los riesgos asociados a la criticidad de los activos de información y a la continuidad de los servicios misionales.

- Finalizar la definición, aprobación e implementación de los indicadores de gestión del MSPI, de manera que se cuente con mecanismos objetivos de medición del avance, desempeño y nivel de madurez del modelo.

- Fortalecer la trazabilidad entre riesgos, controles, planes de tratamiento y acciones de mejora, garantizando evidencia clara del cierre efectivo del ciclo PHVA.

Recomendación 2:

Se recomienda a la OTIC diseñar, formalizar e implementar mecanismos consolidados de medición que permitan evaluar de manera objetiva, periódica y verificable la madurez y efectividad del MSPI, en concordancia con el ciclo PHVA, los lineamientos del MSPI y la norma ISO 27001:2022.

Recomendación 3:

Para los controles que se encuentran en estado “Gestionado” o “Efectivo”, pero sin evidencia de incumplimiento normativo, se recomienda:

- Continuar avanzando hacia la optimización y estandarización documental de los controles nuevos de ISO 27001:2022.

- Actualizar y mantener alineada la Declaración de Aplicabilidad (SoA) con los repositorios institucionales y el estado real de implementación.

- Asegurar que las prácticas operativas estén respaldadas por políticas, procedimientos e instructivos vigentes, publicados y aprobados.

Recomendación 4:

Se recomienda fortalecer y sensibilizar a los servidores públicos, contratistas, terceros, profesores, aprendices, estudiantes, practicantes, usuarios, consultores, ciudadanía, y en general a todas las personas que de manera directa o indirecta hagan uso o utilicen los servicios e infraestructura tecnológica del nivel institucional, local y central de la SED para el acceso y navegación en internet en lo relacionado con el Programa Anual de Pruebas de Intrusión (Ethical Hacking) sobre la infraestructura crítica de la entidad. Esta acción debe contemplar:

- Alcance: Inclusión de aplicaciones core, servicios ciudadanos digitales y bases de datos sensibles.

- Metodología: Adopción de marcos de trabajo reconocidos (como OWASP o OSSTMM) para evaluar la resiliencia frente a accesos no autorizados.

- Remediación: Establecer un flujo de trabajo donde los hallazgos técnicos se integren de forma inmediata a la Matriz de Riesgos de Seguridad Digital y al Plan de Tratamiento de Riesgos, asegurando que la mitigación sea validada en una segunda fase de pruebas ("Retest").

- Alineación: Asegurar que los resultados de estos ejercicios sirvan de insumo para la actualización anual del MSPI conforme a la Resolución 02277 de 2025.

Recomendación 5:

Se recomienda priorizar la culminación de los PM que permanecen abiertos, fortaleciendo la ejecución integral de las acciones formuladas y acordadas en la mesa de trabajo realizada junto a la OCI, mediante acciones que permitan demostrar de manera suficiente, pertinente y verificable la ejecución efectiva y la eficacia operativa de los controles implementados, más allá de la formalización normativa o documental, incluida la actualización de los procedimientos relacionados. Es importante que las acciones, que se consideren cumplidas, cuenten con evidencia de ejecución reportada en el aplicativo ISOLUCION antes de la emisión del informe final de auditoría.

Recomendación 6:

Se recomienda a la OTIC, en articulación con las áreas responsables de la seguridad física y la gestión del riesgo institucional, fortalecer la protección perimetral de los centros de datos, protección contra amenazas físicas y ambientales y la gestión de activos físicos y medios de almacenamiento, considerando las condiciones del entorno y los factores externos de riesgo asociados a su ubicación.

Al respecto, la OCI recomienda:

- Realizar un análisis específico del contexto externo y del entorno de amenazas de cada centro de datos, incorporando variables como afluencia masiva de personas, eventos públicos, condiciones de orden público y riesgos de vandalismo o asonada.

- Evaluar la necesidad de implementar controles de seguridad perimetral reforzados, tales como cerramientos adicionales, barreras físicas especializadas, iluminación perimetral, monitoreo permanente y protocolos de seguridad diferenciados para eventos de alto riesgo.

- Integrar estos controles al Plan de Seguridad Física y al Plan de Continuidad de Servicios TIC, garantizando una respuesta preventiva y coordinada ante escenarios de riesgo externo que puedan afectar la infraestructura crítica.

- Revisar y actualizar el análisis de riesgos físicos y ambientales de los centros de datos, incorporando escenarios relacionados con fallas eléctricas, eventos climáticos extremos, incendios, inundaciones u otras afectaciones externas.

- Evaluar la suficiencia y capacidad de los controles existentes de protección ambiental y de soporte, tales como sistemas contra incendios, climatización, energía regulada, UPS y planes de contingencia, definiendo acciones de mejora o esquemas de redundancia cuando se identifique riesgo residual significativo.

- Alinear estos controles con los planes de continuidad, recuperación y gestión de crisis, asegurando que la infraestructura tecnológica crítica cuente con niveles adecuados de resiliencia operativa frente a interrupciones no previstas.

- Estandarizar y fortalecer los procedimientos asociados al ciclo de vida de los activos físicos, garantizando que la ubicación, protección, mantenimiento, traslado, reutilización y disposición final de los equipos se realicen bajo lineamientos homogéneos en todas las sedes.

- Formalizar y documentar de manera integral los controles relacionados con:

    - Gestión y custodia de medios de almacenamiento.
    - Seguridad del cableado y de los puntos de conexión.
    - Mantenimiento preventivo y correctivo de equipos.
    - Eliminación segura y verificable de la información antes de la baja o reutilización de activos.

- Definir roles y responsabilidades claras entre las áreas involucradas en la gestión de la infraestructura física y establecer mecanismos de seguimiento periódico que permitan verificar la aplicación uniforme de los controles físicos definidos.

Recomendación 7:

Se recomienda integrar los resultados de las pruebas de recorrido a los centros de datos dentro del SGSI, de manera que:

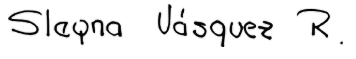
- Las debilidades identificadas en los controles físicos sean incorporadas en la gestión de riesgos de seguridad de la información.

- Las acciones de mejora se prioricen en función de la criticidad de los activos tecnológicos y de los servicios misionales que soporta la infraestructura.

- Se fortalezca la coherencia entre los controles físicos, tecnológicos y organizacionales, en el marco del MSPI y de la ISO 27001:2022, contribuyendo al cierre efectivo de brechas y a la mejora continua del modelo.

V. FIRMAS

Informe elaborado por:



YESID HERNANDO MARÍN CORBA	SLEYNA VÁSQUEZ RODRÍGUEZ
Profesional Especializado - OCI	Profesional Universitario - OCI

HÉCTOR DARÍO TRIANA
Profesional Contratista - OCI

ÓSCAR ALBERTO BARRAGÁN LEÓN
Profesional Contratista - OCI

Informe revisado por:

PABLO EDUARDO GAMBOA TORRES
Profesional Contratista - OCI

Informe aprobado por:

Marlon Enrique Mendez Villamizar

Firmado digitalmente por Marlon Enrique Mendez Villamizar
Fecha: 2026.05.28 12:31:56 -05'00'

MARLON ENRIQUE MÉNDEZ VILLAMIZAR
Jefe Oficina de Control Interno