INFORME DE AUDITORÍA INTERNA BASADA EN RIESGOS
NIVEL CENTRAL
OFICINA DE CONTROL INTERNO

PROCESO Gestión de Servicios TIC	**SUBPROCESO** Sistema De Gestión De Seguridad De La Información (Controles Informáticos)
TIPO DE PROCESO **MISIONAL _____ APOYO** [X] **ESTRATÉGICO _____ EVALUACIÓN Y CONTROL _____**	
ÁREA AUDITADA Equipo de Gestión Estratégica y Seguridad de Información OTI Oficina de Tecnologías de la Información	
UNIDAD AUDITABLE Política de Seguridad y Privacidad de la Información: GIT-PTI-POL-001 V.3 Manual de políticas de Seguridad de la Información.	
TIPO DE AUDITORÍA: **Auditoría Interna** [X] **Auditoría de Cumplimiento ___ Auditoría de seguimiento ____** **Auditorías específicas: ____ Auditorías de sistemas o de TIC: ____¿Cuál? _____**	
LUGAR DE DESARROLLO DE LA AUDITORÍA **Oficinas Nacionales** [X] **Gerencia Seccional ____ Oficina Local ____ PAPF ____ Otro ____ ¿Cuál?_____**	
FORMA DE DESARROLLO DE LA AUDITORÍA: Presencial ____ Remota ____ Mixta [X]	
VIGENCIA: 2024-2025	
FECHA DE INICIO: 27/02/2026	**FECHA DE FINALIZACIÓN:** 30/06/2026

TIPO DE INFORME:	Preliminar _ Definitivo __**[X]**_	Fecha: 30/07/2026

1. OBJETIVO

Evaluar la aplicación, implementación y cumplimiento de la Política de Seguridad y Privacidad de la Información GIT-PTI-POL-001 V.3 Manual de políticas de Seguridad de la Información, en la Oficina de Tecnologías de la Información – OTI, con énfasis en el Equipo de Gestión Estratégica y Seguridad de Información TI, considerando el Modelo de Seguridad y Privacidad de la Información – MSPI, previsto en el Anexo 1 de la Resolución 500 de 2021 y actualizado por la Resolución 2277 de 2025 del MinTIC, así como los controles o requisitos aplicables de la NTC/ISO 27001, para el periodo evaluado 2022 a 2025.

El objetivo de la auditoría no se limita a constatar la existencia formal de la política o de documentos asociados al SGSI/MSPI. La revisión busca establecer, con base en evidencia documental, técnica y administrativa, si los lineamientos de seguridad y privacidad definidos por la entidad se encuentran efectivamente aplicados en los activos de información, servicios digitales, sistemas de información, infraestructura tecnológica, gestión de accesos, operación segura, continuidad, respaldo, gestión de incidentes, gestión de vulnerabilidades, relación con proveedores, contratos tecnológicos y cumplimiento normativo.

En ese sentido, la auditoría pretende verificar si la OTI cuenta con mecanismos institucionales suficientes para demostrar que la política se encuentra incorporada en la gestión operativa de tecnología y seguridad de la información, y si dichos mecanismos permiten preservar la confidencialidad, integridad, disponibilidad, trazabilidad y privacidad de la información institucional.

Asimismo, la auditoría busca analizar la relación entre la política auditada, los riesgos institucionales definidos en la planeación, los controles existentes y las evidencias aportadas por el área auditada. La revisión se orientó a determinar, con base en la evidencia examinada, si los controles implementados mitigan razonablemente los riesgos asociados a la adquisición de bienes y servicios tecnológicos, el cumplimiento de acuerdos de nivel de servicio, la alineación

estratégica de tecnología, la implementación del SGSI/MSPI y la observancia de la normatividad aplicable.

2. ALCANCE

La auditoría comprende la evaluación de la aplicación de la Política de Seguridad y Privacidad de la Información GIT-PTI-POL-001 V.3 Manual de políticas de Seguridad de la Información sobre los activos de información, servicios digitales, sistemas de información e infraestructura tecnológica bajo gestión o administración de la Oficina de Tecnologías de la Información – OTI, en el marco del proceso Gestión de Servicios TIC y del subproceso Gestionar la Seguridad de la Información, controles informáticos.

El alcance de la auditoría cubre el periodo de evidencias comprendido entre las vigencias 2022 a 2025, en relación con la implementación, operación, seguimiento y trazabilidad de los controles de seguridad y privacidad de la información definidos por la entidad. La auditoría se desarrolla en Oficinas Nacionales, bajo modalidad mixta, es decir, mediante actividades documentales, remotas y, cuando corresponda, validaciones o reuniones presenciales o virtuales con los responsables del área auditada.

Dentro del alcance se incluyen, de manera específica, los siguientes componentes:

a) **Gobierno y gestión del MSPI/SGSI**, incluyendo roles, responsabilidades, divulgación, apropiación, declaración de aplicabilidad, excepciones y mecanismos de seguimiento.
b) **Activos de información y activos tecnológicos**, incluyendo matrices de activos, inventarios tecnológicos, catálogo de sistemas, servicios digitales, servidores, equipos de cómputo y elementos de infraestructura relevantes para la operación tecnológica institucional.
c) **Gestión de riesgos de seguridad de la información**, incluyendo matrices de riesgos, riesgos institucionales asociados, controles existentes, planes de tratamiento, seguimiento y evidencia de ejecución.
d) **Gestión de accesos, identidades y cuentas privilegiadas**, incluyendo solicitudes de VPN, controles sobre accesos remotos, procedimiento de cuentas privilegiadas, inventarios de cuentas privilegiadas y evidencias de autorización, revisión o seguimiento.
e) **Criptografía y certificados digitales**, en cuanto a la identificación de aplicaciones, certificados SSL y controles asociados a la protección de comunicaciones y servicios.
f) **Seguridad física y ambiental**, incluyendo política aplicable, registros de acceso a centros de datos o infraestructura crítica, controles físicos y evidencias de acceso o supervisión.
g) **Operación segura**, incluyendo gestión de cambios, restauraciones, respaldos, logs, trazabilidad, monitoreo, gestión de vulnerabilidades, parches y protección contra malware, cuando se haya aportado evidencia suficiente.
h) **Proveedores y contratos tecnológicos**, incluyendo contratos, estudios previos, actas de inicio, acuerdos de confidencialidad, soportes contractuales, obligaciones de seguridad, requisitos de confidencialidad, acuerdos de niveles de servicio y evidencias de supervisión o seguimiento.
i) **Gestión de incidentes y continuidad**, incluyendo registros o soportes de incidentes de seguridad, eventos tecnológicos, incidentes relacionados con página web o canales institucionales, formatos de incidentes, evidencias de atención, estrategia DRP, restauraciones y continuidad operativa.
j) **Cumplimiento legal, contractual y de privacidad**, incluyendo evidencias asociadas a requisitos normativos, contractuales, confidencialidad, tratamiento de información, privacidad y alineación con el MSPI.

La auditoría se desarrolla con base en revisión documental, análisis de evidencias, pruebas selectivas y contraste entre política, riesgos, controles y soportes aportados. En consecuencia, las conclusiones del informe se fundamentan únicamente en la información suministrada y revisada durante la fase de ejecución y en los soportes disponibles al cierre de la etapa de discusión. El alcance no corresponde a una auditoría de certificación ISO/IEC 27001 ni a una

revisión exhaustiva de todos los sistemas, contratos, activos, controles o configuraciones técnicas de la entidad.

El alcance tampoco incluye emitir juicios disciplinarios, fiscales, penales o contractuales. Las observaciones se formulan desde el enfoque de auditoría interna, control interno, gestión de riesgos, seguridad de la información y mejora institucional.

3. LIMITACIONES AL ALCANCE

Durante el desarrollo de la auditoría se identificaron limitaciones que condicionan el nivel de conclusión que puede emitirse sobre el cumplimiento integral de la Política de Seguridad y Privacidad de la Información GIT-PTI-POL-001 V.3 Manual de políticas de Seguridad de la Información, del MSPI y de los controles aplicables de la NTC/ISO 27001. Estas limitaciones no impiden formular observaciones; sin embargo, condicionan el nivel de aseguramiento alcanzado y deben considerarse al interpretar los resultados y conclusiones del informe.

La primera limitación corresponde a la **ausencia de evidencia específica para algunos componentes solicitados durante la fase de ejecución**. En particular, no se aportó documentación para el componente **E2 – Gestión de accesos**, lo que impide verificar de manera integral el ciclo de altas, bajas, modificaciones, autorizaciones, implementación, cierre y revisión periódica de accesos a sistemas, servicios o infraestructura crítica. Se aportaron solicitudes VPN y documentos asociados a cuentas privilegiadas, pero estos soportes no reemplazan la evidencia integral de gestión de accesos requerida.

También se identificó ausencia de evidencia para el componente **H4 – Parches y protección Malware**. En consecuencia, no fue posible verificar reportes de cumplimiento de parches, cobertura de antimalware o EDR, activos pendientes de actualización, excepciones, vulnerabilidades asociadas, responsables de remediación o fechas de cierre. Esta limitación afecta la capacidad de la auditoría para concluir sobre la operación efectiva de controles preventivos frente a código malicioso y vulnerabilidades conocidas.

Respecto del componente **C2 – Plan de Tratamiento de Riesgos**, en la carga inicial de evidencias no se allegó un archivo específico. Posteriormente se aportó el **Plan de Tratamiento de Riesgos 2024** como papel de trabajo, pero no se evidenció trazabilidad completa para las vigencias 2022, 2023, 2024 y 2025, incluyendo responsables, estado de avance, soportes de ejecución, cierres, evaluación de residualidad y seguimiento periódico. Por lo anterior, el análisis de riesgos y tratamiento se considera parcial.

En materia de **activos de información**, se aportó principalmente una matriz correspondiente a la vigencia 2023. No se evidenciaron versiones actualizadas para 2024 y 2025, ni soporte equivalente que demuestre actualización anual, revisión, clasificación, rotulado o trazabilidad de cambios durante todo el periodo auditado. Esta limitación impide concluir plenamente sobre el mantenimiento actualizado de la matriz de activos de información conforme a la política.

Las evidencias técnicas asociadas a logs, archivos de auditoría, registros de sistema, correos en formato .msg, archivos comprimidos, hojas de cálculo y soportes técnicos requieren validación selectiva adicional para confirmar su integridad, periodo cubierto, sistema asociado, responsable, fecha de generación y correspondencia con el control evaluado. Por tanto, la sola existencia de archivos técnicos no permite concluir, sin validación adicional, que el control se encuentre implementado de manera completa, periódica y efectiva.

Otra limitación identificada consiste en que varios soportes fueron aportados **por caso, por evento o por actividad**, pero no mediante matrices consolidadas por control, vigencia, responsable, periodicidad, resultado y cierre. Esta situación se observó, entre otros componentes, en incidentes, gestión de cambios, contratos, restauraciones, vulnerabilidades y cumplimiento normativo. La ausencia de consolidación limita la trazabilidad integral y la verificación de continuidad en la operación de los controles durante todo el periodo 2022–2025.

Asimismo, no se aportó una **matriz integral de requisitos legales, contractuales y de privacidad** aplicable a la OTI, al SGSI y al MSPI, ni una relación consolidada de sistemas o servicios que traten datos personales con sus controles técnicos asociados. En K1 se aportaron soportes contractuales específicos, los cuales resultan útiles para verificar obligaciones particulares, pero no permiten concluir sobre la gestión integral de cumplimiento legal, contractual y privacidad.

Finalmente, parte de la información asociada a cuentas privilegiadas, logs, vulnerabilidades, inventarios, certificados, contratos, configuraciones o sistemas contiene información sensible. Por razones de seguridad, el análisis de auditoría debe limitarse a verificar existencia, formalización, trazabilidad, seguimiento y suficiencia documental, sin reproducir en el informe detalles técnicos que puedan comprometer la seguridad de la entidad.

En consecuencia, las observaciones se mantienen con base en la evidencia disponible al cierre de la auditoría. Durante la etapa de discusión, la OTI no presentó observaciones ni aportó evidencia adicional que modificara las limitaciones descritas.

4. CRITERIOS

Los criterios de auditoría corresponden al conjunto de políticas, normas, procedimientos, controles, documentos institucionales y riesgos frente a los cuales se comparó la evidencia aportada por la Oficina de Tecnologías de la Información. Estos criterios permiten determinar si la aplicación de la Política de Seguridad y Privacidad de la Información GIT-PTI-POL-001 V.3 se encuentra debidamente soportada, implementada, documentada y alineada con el marco institucional y normativo aplicable.

El primer criterio corresponde a la **Política de Seguridad y Privacidad de la Información GIT-PTI-POL-001 V.3** Manual de políticas de Seguridad de la Información, por ser el documento principal objeto de auditoría. Esta política establece lineamientos para la protección de la información institucional y contempla dominios relacionados con autoridades y roles, toma de conciencia, activos de información, activos tecnológicos, control de acceso, criptografía, seguridad física, operación segura, gestión de cambios, copias de respaldo, registros de auditoría, gestión de vulnerabilidades, proveedores, incidentes, continuidad y cumplimiento legal o contractual.

En segundo lugar, se considera el **Modelo de Seguridad y Privacidad de la Información – MSPI**, previsto en el Anexo 1 de la Resolución 500 de 2021 y actualizado por la Resolución 2277 de 2025 del MinTIC, conforme fue definido en la planeación de la auditoría. Este modelo constituye el marco de referencia para evaluar la gestión de seguridad y privacidad de la información en entidades públicas, como habilitador de la Política de Gobierno Digital.

También se consideran como criterio la **Resolución 500 de 2021 del MinTIC** y la **Resolución 2277 de 2025 del MinTIC**, en cuanto establecen y actualizan el marco del MSPI. En particular, la auditoría toma en cuenta que el modelo fue actualizado y que, por tanto, la entidad debe contar con evidencias que permitan demostrar análisis, adopción, ajuste o alineación frente al marco vigente.

La **NTC/ISO 27001** se utiliza como referencia técnica únicamente respecto de los controles o requisitos aplicables al alcance auditado. La auditoría no tiene por objeto certificar el sistema de gestión ni emitir concepto de certificación ISO; la referencia se emplea para contrastar controles relacionados con gobierno, activos, accesos, operación, proveedores, incidentes, continuidad, cumplimiento, riesgos y mejora.

Se incluye como criterio el **Procedimiento CIG-OCI-P-002 – Desarrollo de Auditoría Interna Basada en Riesgos**, por ser el procedimiento institucional que regula el desarrollo de esta auditoría. Este procedimiento orienta la planeación, anuncio, solicitud de información, revisión documental, ejecución, elaboración de papeles de trabajo, emisión de informe preliminar, discusión, contradicción, informe definitivo y seguimiento a planes de mejoramiento.

De igual forma, se consideran los riesgos definidos en la planeación de auditoría y asociados al **Mapa de Riesgos Institucionales V1 2026**, particularmente los riesgos **GTI1, GTI2, GOB1 y GOB2**, relacionados con adquisición de bienes y servicios tecnológicos, prestación de servicios tecnológicos y acuerdos de nivel de servicio, diseño e implementación de planes estratégicos de tecnología, y cumplimiento normativo en la implementación del SGSI/MSPI.

Los riesgos evaluados se relacionan con los siguientes controles existentes definidos en la planeación:

a) Visto bueno técnico del Jefe de OTI, líder técnico y gerente de proyecto frente al cumplimiento de requisitos técnicos antes del traslado a Gestión Contractual;
b) Mantenimiento por proveedores con informe y aval del responsable de plataforma;
c) verificación mensual de capacidad y disponibilidad de sistemas incluidos en los acuerdos de nivel de servicio;
d) Revisión anual del cumplimiento normativo de planes estratégicos y avance de implementación;
e) Participación en mesas de trabajo de seguridad, análisis e implementación de lineamientos impartidos, revisión de cumplimiento de actividades en el marco de Gobierno Digital, seguimiento mensual e implementación anual.

Adicionalmente, se consideran como criterios los documentos institucionales aportados durante la fase de ejecución y como papeles de trabajo, entre ellos: Manual SGSI, Alcance SGSI, Política SGSI, Objetivos SGSI, Principios SGSI, DOFA SGSI, Partes Interesadas SGSI, lineamientos de riesgos de seguridad de la información, guías de administración de riesgos de seguridad digital, planes de tratamiento de riesgos, inventarios, matrices de activos, procedimientos, formatos, contratos, actas, registros de incidentes, evidencias de divulgación, reportes de restauración, logs, registros de vulnerabilidades y demás soportes suministrados.

En este informe, los criterios no se aplicaron de forma aislada. Cada situación observada se analizó relacionando el criterio aplicable, el riesgo institucional asociado, el control esperado, la evidencia revisada y el resultado de la evaluación. Cuando la evidencia no permitió concluir sobre la operación o efectividad de un control, se registró expresamente como evidencia parcial, evidencia insuficiente o información no aportada.

5. DESARROLLO DE LA AUDITORÍA

5.1 METODOLOGÍA

La auditoría se desarrolló bajo un enfoque de auditoría interna basada en riesgos, orientado a verificar la aplicación, implementación y cumplimiento de la Política de Seguridad y Privacidad de la Información GIT-PTI-POL-001 V.3 Manual de políticas de Seguridad de la Información en la Oficina de Tecnologías de la Información – OTI, con énfasis en el Equipo de Gestión Estratégica y Seguridad de Información TI, durante el periodo evaluado 2022 a 2025.

La metodología aplicada consideró el objetivo, alcance, criterios y riesgos definidos en la planeación aprobada, así como las actividades establecidas en el procedimiento institucional **CIG-OCI-P-002 – Desarrollo de Auditoría Interna Basada en Riesgos**. Dicho procedimiento prevé que, en la fase de ejecución, el equipo auditor analice la documentación solicitada, determine muestra cuando haya lugar, solicite documentación adicional para la verificación, efectúe revisión documental conforme a criterios, alcance y normatividad aplicable, genere papeles de trabajo y desarrolle reuniones con el área auditada cuando sea necesario para aclarar inquietudes del proceso.

La metodología se estructuró en las siguientes etapas:

a) Identificación y organización de la información suministrada

Durante la fase de ejecución se recibió información documental, técnica y administrativa remitida por la OTI, organizada por componentes temáticos. La información fue clasificada de acuerdo con el índice suministrado por el área auditada, así:

A. Gobierno MSPI.
B. Inventario tecnológico.
C. Gestión de riesgos.
D. Activos de información.
E. Gestión de accesos.
F. Criptografía.
G. Seguridad física y ambiental.
H. Operación segura.
I. Proveedores y contratos.
J. Incidentes y continuidad.
K. Cumplimiento legal / cumplimiento de políticas.

Esta clasificación permitió organizar los papeles de trabajo por ejes de control, asociar cada evidencia con el criterio aplicable y facilitar la trazabilidad entre la política auditada, los riesgos institucionales, los controles existentes y los resultados de auditoria.

En esta etapa no se asumió que la simple existencia de un archivo demostrara cumplimiento. Cada evidencia fue considerada como insumo sujeto a validación de pertinencia, suficiencia, completitud, vigencia, trazabilidad y relación directa con el control evaluado.

b) Revisión de criterios aplicables

La revisión se efectuó contrastando las evidencias aportadas contra los criterios definidos para la auditoría, principalmente:

- Política de Seguridad y Privacidad de la Información GIT-PTI-POL-001 V.3. Manual de políticas de Seguridad de la Información.
- Modelo de Seguridad y Privacidad de la Información – MSPI.
- Resolución 500 de 2021 del MinTIC.
- Resolución 2277 de 2025 del MinTIC.
- Controles o requisitos aplicables de la NTC/ISO 27001, únicamente dentro del alcance auditado.
- Procedimientos, manuales, formatos, matrices, planes, registros y demás documentos institucionales aportados por la OTI.
- Riesgos institucionales asociados a la unidad auditable: GTI1, GTI2, GOB1 y GOB2.

El análisis se orientó a verificar no solo la existencia documental de políticas, procedimientos o formatos, sino su evidencia de aplicación durante el periodo evaluado. Por tanto, se revisó si los documentos aportados permitían demostrar operación real del control, responsable definido, periodicidad, seguimiento, cierre y relación con los riesgos auditados.

c) Cruce entre riesgo, control, criterio y evidencia

La auditoría se desarrolló mediante una matriz de análisis que relacionó, para cada componente evaluado, los siguientes elementos:

- Riesgo institucional asociado.
- Control esperado o declarado en la planeación.
- Criterio normativo, técnico o procedimental aplicable.
- Evidencia esperada.
- Evidencia efectivamente aportada.
- Análisis de suficiencia.
- Resultado de la evaluación.
- Observación, cuando la evidencia permitió sustentarla, fortaleza o situación sujeta a ampliación.

Este cruce permitió diferenciar entre: cumplimiento evidenciado, evidencia parcial, ausencia de evidencia, oportunidad de mejora y observación preliminar. Cuando la evidencia aportada no permitió concluir cumplimiento o incumplimiento, se dejó expresamente la condición como

“evidencia parcial”, **“información pendiente de validación”** o **“situación sujeta a ampliación de evidencia”**.

d) Revisión documental y técnica por componentes

La revisión documental incluyó el análisis de soportes como políticas, procedimientos, inventarios, matrices, listados, contratos, actas, formatos, reportes, registros de eventos, evidencias de capacitación, soportes de incidentes, restauraciones, logs, reportes de vulnerabilidades y documentos de continuidad.

La revisión técnica se realizó sobre la base de los documentos y archivos suministrados por el área auditada, sin realizar pruebas intrusivas, escaneos independientes, extracción directa de información de sistemas productivos ni auditoría de certificación ISO. En los casos de logs, registros técnicos, inventarios, vulnerabilidades, certificados, cuentas privilegiadas o información sensible, el análisis se limitó a verificar existencia, pertinencia, estructura, trazabilidad documental y correspondencia general con el control evaluado, evitando revelar detalles que pudieran comprometer la seguridad de la entidad.

e) Evaluación de suficiencia y trazabilidad de la evidencia

Para cada grupo de evidencias se aplicaron criterios de evaluación orientados a determinar:

- Si la evidencia correspondía al periodo evaluado 2022–2025.
- Si estaba relacionada con la Política GIT-PTI-POL-001 V.3.
- Si permitía identificar responsable, fecha, sistema, activo, servicio, contrato o proceso asociado.
- Si evidenciaba ejecución del control y no solo diseño documental.
- Si permitía verificar seguimiento, aprobación, cierre o mejora.
- Si cubría el universo o solo casos puntuales.
- Si correspondía a un control preventivo, detectivo, correctivo o de recuperación.
- Si estaba asociada a alguno de los riesgos priorizados en la planeación.

Este análisis permitió establecer que varios controles cuentan con soportes documentales y técnicos; sin embargo, en algunos componentes la evidencia se presentó de forma dispersa, por evento, por caso o por archivo individual, sin consolidación por vigencia, responsable, control, periodicidad, resultado y seguimiento. Esta situación fue considerada en la formulación de observaciones.

f) Solicitud y análisis de información adicional

En la fase de ejecución se solicitó información adicional a la OTI con el fin de complementar la evidencia inicialmente disponible y permitir la verificación de controles relacionados con gobierno MSPI, activos, riesgos, accesos, operación segura, proveedores, incidentes, continuidad y cumplimiento legal. Esta solicitud se efectuó dentro de la fase de ejecución, en concordancia con el procedimiento institucional, que permite solicitar documentación adicional para llevar a cabo la verificación correspondiente.

La información recibida fue incorporada a los papeles de trabajo por bloques temáticos. Aquellos puntos frente a los cuales no se allegó evidencia, o se allegó evidencia parcial, fueron identificados como limitaciones, posibles observaciones o situaciones sujetas a ampliación documental.

g) Elaboración de papeles de trabajo

Los papeles de trabajo fueron estructurados conforme a los componentes evaluados y a las observaciones. Su finalidad fue conservar la trazabilidad entre el requerimiento de auditoría, la evidencia recibida, el criterio aplicado, el análisis efectuado y el resultado preliminar. El procedimiento CIG-OCI-P-002 exige generar papeles de trabajo debidamente señalizados y organizados que evidencien el desarrollo de la auditoría y la aplicación de las técnicas utilizadas.

h) Formulación de resultados de auditoría

Los resultados fueron formulados diferenciando:

- Cumplimiento evidenciado.
- Evidencia parcial.
- Ausencia o insuficiencia de evidencia.
- Fortalezas.
- Observaciones.
- Recomendaciones.
- Limitaciones derivadas de información no aportada.

La formulación de observaciones se realizó cuando existió una diferencia verificable entre el criterio aplicable y la condición encontrada, o cuando la ausencia de evidencia afectó la posibilidad de demostrar la operación de un control relevante.

5.2 MUESTRA

La muestra de auditoría fue definida mediante un criterio **selectivo, dirigido y basado en riesgos**, teniendo en cuenta la naturaleza de la auditoría, el alcance definido en la planeación, los riesgos institucionales asociados, la criticidad de los componentes evaluados y la información efectivamente suministrada por la OTI.

No se aplicó una muestra estadística probabilística, dado que la auditoría no tuvo como finalidad extrapolar resultados cuantitativos a la totalidad de activos, sistemas, contratos, servicios, usuarios o controles de la entidad. La selección se realizó con base en juicio profesional del equipo auditor, priorizando evidencias que permitieran evaluar controles relevantes para la seguridad y privacidad de la información, la continuidad del servicio, la trazabilidad, la gestión de accesos, la operación segura y el cumplimiento normativo.

El procedimiento CIG-OCI-P-002 establece que, una vez analizada la documentación solicitada, se determina la muestra cuando haya lugar; por tanto, para esta auditoría la muestra se definió después de identificar el universo documental y técnico aportado por la OTI.

5.2.1. Criterios utilizados para seleccionar la muestra

La muestra se seleccionó considerando los siguientes criterios:

a) Enfoque basado en riesgos

Se priorizaron evidencias relacionadas con los riesgos institucionales definidos en la planeación de auditoría:

- Riesgo asociado a adquisición de bienes y servicios tecnológicos.
- Riesgo asociado a incumplimiento de acuerdos de nivel de servicio tecnológicos y afectación en la prestación de servicios.
- Riesgo asociado a planes estratégicos de tecnología no conformes con lineamientos vigentes.
- Riesgo asociado a omisión de normatividad aplicable en la implementación del SGSI/MSPI.

Este criterio permitió focalizar la revisión en componentes con mayor exposición frente a confidencialidad, integridad, disponibilidad, continuidad, cumplimiento normativo y prestación de servicios tecnológicos.

b) Cobertura de dominios o componentes de la política

Se seleccionaron evidencias que permitieran cubrir los principales componentes de la Política GIT-PTI-POL-001 V.3 y del MSPI, entre ellos: gobierno de seguridad, activos de información, inventario tecnológico, accesos, cuentas privilegiadas, criptografía, seguridad física, operación

segura, gestión de cambios, respaldos, logs, vulnerabilidades, proveedores, incidentes, continuidad y cumplimiento legal.

c) Criticidad tecnológica y operativa

Se priorizaron evidencias asociadas a sistemas, servicios, infraestructura, servidores, contratos o controles que inciden directamente en la disponibilidad, continuidad, trazabilidad, seguridad técnica o cumplimiento normativo de la OTI.

d) Periodo evaluado

La muestra consideró evidencias correspondientes al periodo 2022–2025. Cuando la evidencia no cubrió la totalidad del periodo, se registró la limitación correspondiente. En algunos componentes se observó mayor concentración de soportes en las vigencias 2023, 2024 y 2025, por lo cual las conclusiones se formularon de manera prudente y sin extenderlas automáticamente a todo el periodo auditado.

e) Disponibilidad y suficiencia de evidencia

Se seleccionaron los documentos y registros efectivamente aportados por la OTI. Cuando un componente no tuvo evidencia, o la evidencia fue incompleta, el punto se registró como ausencia o insuficiencia de evidencia, sin presumir incumplimiento material del control.

5.2.2. Muestra revisada por componente

La muestra documental y técnica incluyó los siguientes grupos de evidencia:

A. Gobierno MSPI

Se revisaron evidencias de divulgación y apropiación, tales como materiales de sensibilización, presentaciones, reportes de asistencia, cronogramas, charlas, piezas de comunicación y documentos relacionados con phishing, ingeniería social, navegación segura, correo electrónico, documentos físicos, copias de seguridad, incidentes de seguridad, redes sociales, medios extraíbles y hábitos en el puesto de trabajo.

También se revisó la información aportada sobre roles y responsabilidades de la OTI, así como la Declaración de Aplicabilidad 2023 presentada como soporte del componente de excepciones o aplicabilidad.

B. Inventario tecnológico

Se revisaron catálogos de sistemas y servicios, inventario tecnológico a nivel nacional e inventario de servidores. Estos documentos fueron considerados relevantes para identificar el universo tecnológico sobre el cual se aplica la política auditada.

C. Gestión de riesgos

Se revisó la matriz consolidada de riesgos de seguridad de la información y el Plan de Tratamiento de Riesgos 2024 aportado como papel de trabajo. No se contó inicialmente con evidencia completa para el componente C2, por lo cual el análisis del tratamiento de riesgos se consideró parcial.

D. Activos de información

Se revisó la matriz de activos de información correspondiente a 2023. Esta evidencia fue utilizada para verificar la existencia de un instrumento de identificación de activos; sin embargo, no permitió concluir actualización anual para 2024 y 2025.

E. Gestión de accesos

Se revisaron solicitudes VPN y documentos asociados a cuentas privilegiadas, incluyendo el procedimiento GIT-PTI-P-002 y las formas institucionales 4-1044 y 4-1045. No se contó con evidencia para el componente E2 – Gestión de accesos, razón por la cual no fue posible verificar integralmente altas, bajas, modificaciones, recertificaciones y cierres de accesos.

F. Criptografía

Se revisaron listados de aplicaciones y relación de certificados SSL de aplicaciones misionales. Estos soportes fueron utilizados para verificar la existencia de información base sobre mecanismos criptográficos asociados a servicios y aplicaciones.

G. Seguridad física y ambiental

Se revisó la política de seguridad y evidencias de registros de acceso a datacenter o infraestructura crítica, incluyendo informe de accesos e informe de proveedor.

H. Operación segura

Se revisaron evidencias de gestión de cambios, incluyendo procedimiento, solicitudes, aprobaciones, minutogramas, pruebas, vistos buenos y documentos asociados a pasos a producción o ajustes tecnológicos. También se revisaron soportes de restauraciones y backup, evidencias de logs y trazabilidad, configuración de tiempo, monitoreo, disponibilidad y respaldo, así como reportes de análisis de vulnerabilidades y mitigación. Para H4 – Parches y protección malware no se aportó evidencia, por lo que dicho componente quedó registrado como limitación y dio lugar a la Observación 05.

I. Proveedores y contratos

Se revisaron contratos, estudios previos, actas de inicio, soportes contractuales y acuerdo de confidencialidad asociados a servicios tecnológicos, ciberseguridad, infraestructura y SOC. La muestra permitió identificar evidencia contractual relevante, aunque no permitió concluir seguimiento integral de ANS/SLA, obligaciones de seguridad y supervisión de controles por contrato.

J. Incidentes y continuidad

Se revisaron documentos asociados a incidentes o eventos tecnológicos relacionados con página web institucional, Google Search Console, DNS, cuenta institucional de YouTube, formatos de incidentes y comunicaciones de soporte. Para continuidad se revisó la Estrategia DRP – ICA Preliminar y evidencias de restauración aportadas en H2.

K. Cumplimiento legal / cumplimiento de políticas

Se revisaron soportes contractuales específicos asociados a estudio previo, contrato, acuerdo de confidencialidad y acta de inicio. Estos documentos fueron útiles para verificar obligaciones particulares, pero no reemplazan una matriz integral de requisitos legales, contractuales y de privacidad aplicable al SGSI/MSPI.

5.2.3. Forma de cálculo de la muestra

La muestra fue calculada mediante selección dirigida por riesgo, cobertura temática y disponibilidad de evidencia. No se utilizó fórmula estadística, debido a que el universo de auditoría estaba conformado por documentos, soportes técnicos, contratos, registros y evidencias heterogéneas, y porque el objetivo de la auditoría fue verificar la aplicación de controles críticos frente a la política auditada, no estimar porcentajes de cumplimiento sobre una población homogénea.

La selección se consideró apropiada en la medida en que permitió cubrir los componentes principales del alcance: activos de información, servicios digitales, sistemas, infraestructura, accesos, operación segura, continuidad, incidentes, contratos y cumplimiento normativo. No

obstante, se deja constancia de que la muestra no agota la totalidad del universo de sistemas, activos, contratos, usuarios, logs, vulnerabilidades, respaldos o incidentes de la OTI.

Por lo anterior, las conclusiones del informe se limitan a la muestra y a la evidencia efectivamente revisada, sin extenderse a elementos que no fueron incluidos en la muestra o que no fueron suministrados durante la ejecución y discusión de la auditoría.

5.3 FORTALEZAS

De acuerdo con el procedimiento institucional, las fortalezas corresponden a aspectos positivos o buenas prácticas que contribuyen al cumplimiento de los objetivos de la auditoría. En esta auditoría, las fortalezas se formulan únicamente sobre evidencias aportadas por la OTI y no implican, por sí mismas, una conclusión de cumplimiento integral de la Política GIT-PTI-POL-001 V.3, del MSPI o de la NTC/ISO 27001.

Fortaleza 1. Evidencias de actividades de divulgación y apropiación en seguridad de la información
Se identificó un conjunto amplio de materiales y soportes orientados a la sensibilización de usuarios en temas de seguridad de la información, tales como phishing, ingeniería social, navegación segura, correo electrónico, copias de seguridad, incidentes de seguridad, redes sociales, documentos físicos, medios extraíbles, uso de memorias flash y hábitos seguros en el puesto de trabajo.

Estos soportes evidencian que la OTI ha desarrollado actividades de comunicación y toma de conciencia en diferentes temas relacionados con el uso seguro de la información y de los recursos tecnológicos. La existencia de presentaciones, cronogramas, reportes de asistencia, piezas de comunicación y registros de charlas contribuye a demostrar acciones de apropiación de cultura de seguridad, aspecto relevante para el MSPI y para la implementación de la política auditada.

Esta fortaleza es relevante porque la toma de conciencia reduce la exposición a errores humanos, ingeniería social, uso inadecuado de medios extraíbles, manejo inseguro del correo electrónico y reporte tardío de incidentes.

Fortaleza 2. Existencia de documentación institucional del SGSI/MSPI y política objeto de auditoría
Se aportaron documentos relacionados con el SGSI/MSPI, tales como política, manual, alcance, objetivos, principios, DOFA, partes interesadas, lineamientos de riesgos, guías de administración de riesgos y documentos normativos de referencia. La existencia de estos documentos permite contar con una base formal para orientar la gestión de seguridad y privacidad de la información en la entidad.

Esta fortaleza no implica que todos los lineamientos estén plenamente implementados; sin embargo, sí evidencia que la entidad cuenta con un marco documental que puede ser utilizado para definir responsabilidades, controles, riesgos, seguimiento, actualización normativa y mejora continua.

Fortaleza 3. Existencia de inventarios y catálogos para identificar el universo tecnológico
La OTI aportó catálogos de sistemas y servicios, inventario tecnológico a nivel nacional e inventario de servidores. Estos documentos son relevantes porque permiten identificar parte del universo tecnológico sobre el cual deben aplicarse los controles de seguridad y privacidad de la información.

La disponibilidad de inventarios y catálogos facilita la identificación de sistemas, servicios, equipos, servidores, componentes tecnológicos y posibles dependencias. Esta información es necesaria para planear controles, priorizar activos críticos, definir muestras de auditoría, asociar sistemas a riesgos, gestionar vulnerabilidades, respaldos, continuidad y responsabilidades técnicas.

Fortaleza 4. Existencia de procedimiento y formatos para la gestión de cuentas privilegiadas
Se identificó la existencia del procedimiento **GIT-PTI-P-002 – Cuentas Privilegiadas V2** y de las formas institucionales asociadas al inventario y formato de cuentas privilegiadas. Este elemento constituye una fortaleza porque las cuentas privilegiadas representan un punto crítico de control en seguridad de la información, debido a que permiten ejecutar acciones administrativas, modificar configuraciones, acceder a información sensible o afectar la operación de sistemas.

Contar con un procedimiento y formatos específicos permite estructurar la identificación, registro, control y revisión de este tipo de cuentas. Aunque el informe mantiene observación frente a la gestión integral de accesos, la existencia de este procedimiento constituye un avance concreto frente al control de privilegios.

Fortaleza 5. Evidencias de solicitudes VPN y control documental de accesos remotos
Se aportaron varias solicitudes VPN en formato documental. Estas evidencias permiten observar que determinados accesos remotos fueron gestionados mediante formatos o solicitudes, lo cual aporta trazabilidad sobre usuarios, finalidades, aprobaciones o soportes requeridos para acceso remoto.

La gestión formal de solicitudes VPN es relevante porque el acceso remoto constituye un vector de riesgo para la infraestructura tecnológica. La existencia de soportes documentales contribuye a demostrar que, al menos en los casos revisados, se documentó una solicitud de acceso y se conservó evidencia asociada.

Esta fortaleza debe leerse de manera complementaria con la observación sobre gestión integral de accesos, dado que las solicitudes VPN no sustituyen la evidencia completa de altas, bajas, modificaciones, recertificaciones y cierre de accesos a sistemas críticos.

Fortaleza 6. Existencia de procedimiento y soportes de gestión de cambios
Se aportó el procedimiento de gestión de cambios y un número significativo de evidencias asociadas a solicitudes, aprobaciones, minutogramas, vistos buenos, pruebas funcionales, pasos a producción y comunicaciones relacionadas con cambios tecnológicos.

La gestión de cambios es un control relevante para la operación segura, porque permite reducir riesgos derivados de modificaciones no autorizadas, fallas en producción, indisponibilidad, pérdida de trazabilidad o cambios sin evaluación de impacto. La existencia de procedimiento y soportes documentales muestra que la OTI cuenta con mecanismos para formalizar y documentar cambios sobre sistemas, aplicaciones o infraestructura.

Esta fortaleza contribuye a la disponibilidad, estabilidad y trazabilidad de los servicios tecnológicos, aunque no elimina la necesidad de verificar, en cada caso, que los cambios cuenten con evaluación de impacto, plan de reversa, pruebas, aprobación, cierre y registro completo.

Fortaleza 7. Evidencias de restauraciones y respaldos sobre algunos sistemas
Se aportaron soportes de restauraciones y backup asociados a sistemas como Novasoft, SIGMA, SimplifICA y otros documentos relacionados. Esta evidencia es relevante porque demuestra actividades puntuales de recuperación o restauración, las cuales son esenciales para preservar la disponibilidad de información y servicios tecnológicos.

La existencia de pruebas o registros de restauración permite verificar que, para determinados casos, la entidad ejecutó actividades orientadas a validar la recuperabilidad de información. Esta fortaleza contribuye al control de continuidad y disponibilidad, especialmente frente a fallas, incidentes o pérdida de información.

No obstante, esta fortaleza no equivale por sí sola a contar con un DRP completo, aprobado y probado para todos los servicios críticos. Por ello se mantiene separada la observación relacionada con continuidad tecnológica y DRP.

Fortaleza 8. Evidencias de logs, monitoreo, trazabilidad técnica y configuración de tiempo
La OTI aportó archivos de logs, evidencia de configuración de tiempo AD/NTP y documentos asociados a monitoreo, disponibilidad y respaldo. Estos soportes evidencian que existen fuentes técnicas de registro y trazabilidad para algunos sistemas o componentes.

La disponibilidad de logs y sincronización horaria constituye una base importante para la investigación de incidentes, reconstrucción de eventos, verificación de acciones administrativas, análisis de fallas y control de trazabilidad. La evidencia aportada demuestra que existen registros técnicos que pueden ser utilizados como insumo de auditoría o de investigación interna.

Esta fortaleza se presenta sin perjuicio de la observación sobre la necesidad de formalizar un esquema consolidado de gestión de logs, retención, protección, acceso y revisión periódica.

Fortaleza 9. Evidencias de análisis de vulnerabilidades y fase de mitigación
Se aportaron reportes de análisis de vulnerabilidades, informes finales, consolidado de vulnerabilidades y documentos relacionados con fase de mitigación. Estos soportes evidencian que la OTI ha desarrollado actividades de identificación técnica de debilidades sobre infraestructura, servicios o aplicaciones.

El análisis de vulnerabilidades constituye un control relevante para anticipar riesgos, priorizar acciones de remediación, reducir exposición técnica y fortalecer la postura de seguridad. La existencia de reportes y documentos de mitigación permite identificar un proceso orientado a evaluar debilidades y gestionar acciones correctivas o de reducción de riesgo.

La fortaleza se limita a la evidencia aportada; la efectividad del control depende de que las vulnerabilidades cuenten con priorización, responsables, fechas de cierre, evidencia de remediación y aceptación formal del riesgo cuando corresponda.

Fortaleza 10. Existencia de soportes contractuales asociados a servicios tecnológicos y ciberseguridad
Se aportaron contratos, actas de inicio, estudios previos, acuerdos de confidencialidad y documentos contractuales relacionados con servicios tecnológicos, infraestructura, SOC y ciberseguridad. Estos soportes evidencian que la OTI conserva documentación contractual relevante para servicios que pueden incidir en la implementación u operación de controles de seguridad de la información.

La existencia de acuerdos de confidencialidad, estudios previos y contratos permite verificar que algunos servicios tecnológicos cuentan con soporte contractual y obligaciones documentadas. Esto contribuye a la trazabilidad de responsabilidades entre la entidad y sus proveedores.

Esta fortaleza no implica que se haya verificado integralmente el cumplimiento de todos los ANS/SLA, obligaciones de seguridad, informes de supervisión o controles pactados; por ello, se mantiene la observación sobre la necesidad de consolidar seguimiento contractual de controles de seguridad y niveles de servicio.

Fortaleza 11. Evidencias de atención documental de incidentes específicos
Se aportaron soportes relacionados con incidentes o eventos asociados a la página web institucional, Google Search Console, DNS y cuenta institucional de YouTube, así como formatos de incidentes de seguridad. Esta información muestra que algunos eventos fueron documentados y atendidos mediante comunicaciones, revisiones técnicas o registros asociados.

La existencia de soportes por caso contribuye a la trazabilidad de eventos relevantes y permite observar que la OTI conserva evidencia sobre actuaciones desarrolladas frente a situaciones de seguridad o disponibilidad. Esta fortaleza es relevante para la gestión de incidentes, aunque no reemplaza la necesidad de contar con un registro consolidado de incidentes para todo el periodo evaluado.

Fortaleza 12. Existencia de una estrategia preliminar de recuperación ante desastres
Se aportó una estrategia DRP preliminar. Este documento evidencia un avance en la estructuración de mecanismos de recuperación ante desastres y continuidad tecnológica. Su

existencia es relevante porque permite identificar que la entidad ha iniciado o documentado un enfoque para tratar escenarios de recuperación.

No obstante, al tratarse de una estrategia preliminar, no permite concluir que exista un DRP final, aprobado, probado y mantenido para los servicios críticos. Por tanto, se registra como fortaleza en términos de avance documental, pero se mantiene la observación relacionada con la necesidad de formalizar, aprobar y probar el DRP.

5.4 RESULTADOS

El Informe Preliminar de Auditoría fue remitido a la Oficina de Tecnologías de la Información – OTI mediante memorando radicado **20263015843** del 14 de julio de 2026, para su revisión, contradicción y aporte de evidencias adicionales. Otorgando el término de cinco (5) días hábiles para presentar observaciones, comentarios o evidencias adicionales. Vencido dicho término, no se recibió respuesta por parte del área auditada. En consecuencia, de acuerdo con el Procedimiento CIG-OCI-P-002, se da por surtida la etapa de discusión, el informe queda en firme, las diez observaciones y sus correspondientes recomendaciones se mantienen sin modificación y el presente documento se emite como Informe Definitivo de Auditoría.

Observación 01. Evidencia insuficiente sobre la formalización y trazabilidad de los roles operativos de seguridad de la información.
Como resultado de la revisión del componente **A2 – Roles y responsabilidades OTI**, se identificó que la Oficina de Tecnologías de la Información cuenta con funciones asociadas a la seguridad de la información, gestión de accesos, gestión de vulnerabilidades, copias de respaldo, gestión de incidentes, monitoreo, continuidad y supervisión contractual. Sin embargo, la evidencia aportada no permite verificar una matriz formal, vigente, integral y trazable que asigne responsabilidades específicas por control, actividad, dominio o componente del SGSI/MSPI.

La información revisada evidencia una asignación funcional de responsabilidades por grupos o perfiles; no obstante, no se observa con suficiente claridad quién es responsable de ejecutar, aprobar, revisar, monitorear, escalar y reportar cada control relacionado con la Política GIT-PTI-POL-001 V.3. Tampoco se evidenciaron suplencias, periodicidad de seguimiento, autoridad asignada, mecanismo de rendición de cuentas, evidencia esperada por actividad ni relación directa entre los responsables definidos y los controles de la política.

Esta situación limita la trazabilidad del gobierno de seguridad de la información, especialmente en componentes críticos como accesos, cuentas privilegiadas, vulnerabilidades, respaldos, logs, incidentes, continuidad, contratos y cumplimiento normativo. Desde el enfoque de auditoría basada en riesgos, un control puede existir documentalmente, pero su efectividad se dificulta cuando no se identifica de manera clara quién responde por su ejecución, seguimiento y mejora.

Criterio: Política de Seguridad y Privacidad de la Información GIT-PTI-POL-001 V.3 Manual de políticas de Seguridad de la Información; MSPI; documentos institucionales del SGSI; requerimiento de información A2; riesgos asociados a implementación del SGSI/MSPI.
Evidencia revisada: Información roles y responsabilidades OTI.pdf.

Riesgo asociado: GOB2 – posibilidad de afectación reputacional por sanciones debido a omisión de normatividad aplicable en la implementación del Sistema de Gestión de Seguridad de la Información.

Efecto o riesgo: La ausencia de trazabilidad formal de roles puede generar debilidades en la operación, seguimiento y rendición de cuentas sobre controles de seguridad, así como dificultad para establecer responsables frente a incidentes, fallas de control, incumplimientos o acciones de mejora.

Recomendación 01

Formalizar una matriz integral de roles y responsabilidades de seguridad de la información, asociada a la Política GIT-PTI-POL-001 V.3 Manual de políticas de Seguridad de la Información.,

al MSPI y a los controles aplicables de la NTC/ISO 27001. Esta matriz debería incluir, como mínimo: proceso o dominio de control, actividad, responsable funcional, responsable operativo, responsable de aprobación, suplente, periodicidad de ejecución, evidencia esperada, mecanismo de seguimiento, ruta de escalamiento y relación con los riesgos institucionales aplicables.

Adicionalmente, se recomienda actualizar dicha matriz periódicamente y socializarla con los responsables asignados, de forma que exista trazabilidad entre el control definido, el responsable de ejecución, la evidencia generada y el seguimiento realizado.

Observación 02. Soporte documental insuficiente para evidenciar la actualización de la Declaración de Aplicabilidad y del registro de excepciones en concordancia con el MSPI vigente
En el componente **A3 – Registro de excepciones**, se aportó como evidencia la **Declaración de Aplicabilidad 2023**. No obstante, no se evidenció un registro consolidado de excepciones, exclusiones, dispensas o aceptaciones de riesgo frente a la Política GIT-PTI-POL-001 V.3 para el periodo evaluado 2022–2025.
Tampoco se identificó evidencia suficiente de actualización de la declaración de aplicabilidad frente al marco vigente del MSPI actualizado por la Resolución 2277 de 2025 del MinTIC, ni frente a los controles aplicables de la NTC/ISO 27001 bajo la versión vigente aplicable al modelo. Esta condición es relevante porque la declaración de aplicabilidad debe permitir determinar qué controles son aplicables, cuáles no, cuál es la justificación de exclusión, quién aprueba dicha decisión, qué controles compensatorios existen y cómo se realiza el seguimiento.

La existencia de una declaración de aplicabilidad correspondiente a 2023 constituye un insumo relevante; sin embargo, por sí sola no permite verificar que el SGSI/MSPI haya sido actualizado y ajustado frente al marco normativo vigente para 2025, ni que las excepciones o no aplicabilidades hayan sido formalmente justificadas, aprobadas y monitoreadas durante todo el periodo auditado.

Criterio: Resolución 500 de 2021; Resolución 2277 de 2025 del MinTIC; MSPI; Política GIT-PTI-POL-001 V.3; controles aplicables de la NTC/ISO 27001; requerimiento A3.

Evidencia revisada: OTI-2023-Declaración de Aplicabilidad.xlsx.

Riesgo asociado: GOB2 – posibilidad de afectación reputacional por sanciones debido a omisión de normatividad aplicable en la implementación del SGSI/MSPI.

Efecto o riesgo: La falta de actualización y trazabilidad de la declaración de aplicabilidad puede generar desalineación entre los controles implementados y el marco normativo vigente; además, puede dificultar la identificación de controles no aplicados, excepciones no aprobadas o riesgos aceptados sin la debida formalización.

Recomendación 02
Actualizar la declaración de aplicabilidad del SGSI/MSPI, incorporando la trazabilidad frente a la Política GIT-PTI-POL-001 V.3, el MSPI actualizado, la Resolución 2277 de 2025 y los controles aplicables de la NTC/ISO 27001. Esta actualización debería incluir: control, aplicabilidad, justificación, evidencia asociada, responsable, estado de implementación, exclusiones, controles compensatorios, aceptación de riesgos y aprobación correspondiente.

De igual forma, se recomienda implementar y mantener un registro formal de excepciones, dispensas, exclusiones o aceptaciones de riesgo frente a la política y los controles de seguridad, indicando fecha, sistema o proceso afectado, justificación, riesgo asociado, vigencia, responsable, aprobador y controles compensatorios.

Observación 03. No se evidenció la actualización anual de la matriz de activos de información para las vigencias 2024 y 2025.
Para el componente **D1 – Matriz de activos de información**, se aportó una matriz correspondiente a la vigencia 2023. Adicionalmente, se recibieron inventarios tecnológicos, catálogos de sistemas, servicios y servidores. Estos soportes permiten evidenciar que la OTI

cuenta con información base sobre activos, servicios y componentes tecnológicos; sin embargo, no se aportaron versiones actualizadas de la matriz de activos de información para las vigencias 2024 y 2025, ni una versión vigente que demuestre actualización anual.

La Política GIT-PTI-POL-001 V.3 establece la necesidad de identificar y clasificar los activos de información, así como mantener actualizada la matriz correspondiente. En ese sentido, la matriz de activos debe permitir reconocer el activo, propietario, custodio, clasificación, criticidad, ubicación, sistema asociado, fecha de actualización y demás atributos requeridos para aplicar controles proporcionales al nivel de sensibilidad, criticidad y exposición de la información.

La evidencia aportada permite verificar la existencia de una matriz 2023; sin embargo, no permite concluir que durante 2024 y 2025 se haya realizado actualización, revisión, clasificación, rotulado o validación de cambios de los activos de información. Esta condición limita la capacidad de la auditoría para verificar si los controles de confidencialidad, integridad, disponibilidad, retención, respaldo, acceso y tratamiento se aplican sobre una base de activos vigente.

Criterio: Política GIT-PTI-POL-001 V.3; MSPI; controles relacionados con inventario, clasificación y manejo de activos de información; requerimiento D1.

Evidencia revisada: 3 ACTIVOS DE INFORMACION ICA 2023_.xlsx; catálogos de sistemas y servicios; inventario tecnológico nacional; listado de servidores.

Riesgos asociados: GOB2 y GTI2.

Efecto o riesgo: La falta de evidencia de actualización anual puede generar desconocimiento de activos nuevos, retirados, modificados o reclasificados, lo que afecta la aplicación de controles de seguridad y privacidad adecuados.

Recomendación 03
Actualizar y formalizar la matriz de activos de información para las vigencias 2024, 2025 y la vigencia actual, incorporando como mínimo: nombre del activo, descripción, propietario, custodio, clasificación, criticidad, ubicación, repositorio o sistema asociado, tratamiento de datos personales si aplica, controles asignados, fecha de última actualización y responsable de validación.

Se recomienda establecer un procedimiento o cronograma de actualización periódica que permita evidenciar revisión anual, cambios en activos, nuevas adquisiciones, retiro de activos, reclasificaciones y validación por los propietarios de la información.

Observación 04. Evidencia insuficiente de gestión integral de accesos e identidades.
En el componente de gestión de accesos se aportaron solicitudes VPN y documentación asociada a cuentas privilegiadas, incluyendo procedimiento y formatos institucionales. Estos soportes permiten verificar algunos casos de acceso remoto y la existencia de un procedimiento específico para cuentas privilegiadas. Sin embargo, no se aportó evidencia suficiente para el componente **E2 – Gestión de accesos**, relacionado con el ciclo completo de altas, bajas, modificaciones, autorizaciones, implementación, cierre y revisión periódica de accesos.

La evidencia de solicitudes VPN no permite concluir por sí sola sobre la gestión integral de accesos a sistemas, servicios digitales, infraestructura, bases de datos, plataformas críticas o ambientes productivos. Tampoco se aportó muestra suficiente de casos completos que permitan seguir la trazabilidad desde la solicitud hasta la aprobación, creación o modificación del acceso, notificación, uso autorizado, revisión periódica y retiro cuando el acceso deja de ser necesario.

Adicionalmente, no se evidenció recertificación o revisión periódica de accesos para el periodo evaluado. Esta verificación es necesaria para confirmar que los usuarios mantienen únicamente los privilegios requeridos, que los accesos de funcionarios, contratistas o terceros se retiran oportunamente y que no permanecen cuentas activas sin justificación vigente.

Criterio: Política GIT-PTI-POL-001 V.3; procedimiento GIT-PTI-P-002 Cuentas Privilegiadas V2; controles aplicables de acceso lógico, cuentas privilegiadas, VPN y revisión periódica de accesos; requerimientos E1, E2 y E4.

Evidencia revisada: solicitudes VPN; FORMA 4-1044 V.1 Inventario Cuentas Privilegiadas; FORMA 4-1045 V.1 Formato de Cuentas Privilegiadas; GIT-PTI-P-002 Cuentas Privilegiadas V2. No se aportó evidencia para E2.

Riesgos asociados: GTI2 y GOB2.

Efecto o riesgo: La falta de evidencia integral sobre gestión de accesos puede generar permanencia de usuarios con permisos no requeridos, accesos no revocados oportunamente, privilegios excesivos, baja trazabilidad de autorizaciones y exposición a accesos no autorizados.

Recomendación 04
Consolidar e implementar evidencia integral de gestión de accesos, incluyendo procedimiento, matriz de perfiles, solicitudes, aprobaciones, creación, modificación, suspensión, retiro, revisión periódica y cierre de accesos. La evidencia debería permitir verificar, para cada caso, usuario, sistema, perfil, justificación, aprobador, fecha de autorización, fecha de implementación, responsable técnico y estado del acceso.

Se recomienda realizar recertificaciones periódicas de accesos a sistemas críticos, cuentas privilegiadas, cuentas de servicio, VPN y accesos de terceros, dejando evidencia de revisión, ajustes, revocaciones y responsables.

Observación 05. No se aportó evidencia para verificar la gestión de parches y protección contra malware.
Para el componente **H4 – Parches y protección Malware**, no se allegaron soportes documentales o técnicos. En consecuencia, no fue posible verificar la existencia de reportes de cumplimiento de parches, actualización de servidores y estaciones, cobertura de antimalware o EDR, tratamiento de excepciones, vulnerabilidades pendientes, responsables de remediación, fechas de cierre o seguimiento periódico.

La Política GIT-PTI-POL-001 V.3 Manual de políticas de Seguridad de la Información contempla controles orientados a la protección contra código malicioso y a la aplicación de actualizaciones de seguridad. Estos controles son esenciales para reducir la exposición a vulnerabilidades conocidas, ataques automatizados, malware, explotación de sistemas desactualizados, accesos no autorizados y afectación de la disponibilidad de servicios tecnológicos.

La ausencia de evidencia no permite afirmar que el control sea inexistente; sin embargo, desde la perspectiva de auditoría, un control que no cuenta con soporte documental, reportes de ejecución, cobertura, periodicidad y seguimiento no puede considerarse demostrado. Esta situación impide evaluar la efectividad del control durante el periodo auditado.

Criterio: Política GIT-PTI-POL-001 V.3; controles de operación segura, protección contra código malicioso y actualización de parches; controles aplicables de NTC/ISO 27001; requerimiento H4.

Evidencia revisada: No se aportó documentación para H4.

Riesgos asociados: GTI2 y GOB2.

Efecto o riesgo: La falta de evidencia impide verificar si servidores, estaciones, sistemas o componentes tecnológicos se encuentran protegidos frente a malware y vulnerabilidades conocidas. Esto puede aumentar la exposición a incidentes de seguridad, indisponibilidad, pérdida de información o explotación de fallas técnicas.

Recomendación 05
Aportar, consolidar o implementar reportes periódicos de gestión de parches y protección contra malware, diferenciando servidores, estaciones de trabajo, sistemas críticos, dispositivos

tecnológicos y componentes administrados por terceros. Estos reportes deberían incluir cobertura, estado de actualización, fecha del último parche, criticidad, excepciones, vulnerabilidades asociadas, responsable de remediación y fecha de cierre.

Se recomienda definir una periodicidad formal de revisión, establecer indicadores de cumplimiento, documentar excepciones y relacionar la gestión de parches con los resultados de análisis de vulnerabilidades.

Observación 06. Gestión de logs y trazabilidad sin un esquema consolidado de control y con evidencia técnica parcial.
Para el componente **H3 – Gestión de logs y trazabilidad**, la OTI aportó archivos de logs técnicos, evidencia de configuración de tiempo AD/NTP y documentos relacionados con monitoreo, disponibilidad y respaldo. Estos soportes evidencian la existencia de registros técnicos en algunos sistemas o componentes.

Sin embargo, no se evidenció un documento consolidado que defina el esquema institucional de gestión de logs. No se identificó una matriz o procedimiento que precise, para los sistemas críticos: qué eventos se registran, dónde se almacenan, por cuánto tiempo se conservan, quién puede acceder a ellos, cómo se protege su integridad, cómo se revisan, qué eventos generan alerta, quién analiza las alertas y cómo se documentan las acciones derivadas.

La existencia de archivos de logs es un elemento positivo, pero no demuestra por sí sola un control integral de trazabilidad. Para que el control sea verificable, se requiere conocer alcance, responsables, retención, protección contra alteración, acceso autorizado, revisión periódica y tratamiento de eventos. Sin esta formalización, se dificulta reconstruir incidentes, verificar acciones administrativas, soportar investigaciones internas y demostrar integridad de la evidencia técnica.

Criterio: Política GIT-PTI-POL-001 V.3; controles sobre registros de auditoría, protección de logs, sincronización horaria y trazabilidad; requerimiento H3.

Evidencia revisada: cron.log; mysqlerror.log; syslogfe.log.txt; auditdb.log; auditfe.log; EvidenciaConfiguracionTiempoADvsNTP.rtf; Evidencias de monitoreo, disponibilidad y respaldo del sistema SimplifICA.docx.

Riesgos asociados: GTI2 y GOB2.

Efecto o riesgo: La ausencia de un esquema formal de logs puede limitar la capacidad institucional para detectar eventos relevantes, reconstruir incidentes, validar responsabilidades, proteger evidencia digital y responder ante eventos de seguridad o indisponibilidad.

Recomendación 06
Formalizar un procedimiento o matriz de gestión de logs y trazabilidad que incluya fuentes de registro, sistemas cubiertos, eventos mínimos, ubicación de almacenamiento, responsables, retención, controles de acceso, mecanismos de protección contra alteración, sincronización horaria, revisión periódica, alertas, escalamiento y tratamiento de eventos relevantes.
Se recomienda priorizar sistemas críticos, servicios digitales, infraestructura de seguridad, bases de datos, cuentas privilegiadas y componentes expuestos, y vincular esta gestión con incidentes, monitoreo, auditoría técnica y análisis forense cuando aplique.

Observación 07. Estrategia DRP y continuidad tecnológica en estado preliminar, sin evidencia suficiente de implementación y pruebas periódicas.

Para el componente **J2 – Continuidad DRP**, se aportó una **Estrategia DRP – ICA Preliminar**. Adicionalmente, en el componente H2 se aportaron evidencias de restauraciones y respaldos sobre algunos sistemas. Estos soportes permiten identificar avances en actividades de recuperación y respaldo.

No obstante, no se evidenciaron planes DRP finales, aprobados y vigentes por servicios o sistemas de alto impacto. Tampoco se identificaron resultados de pruebas periódicas de continuidad o recuperación durante el periodo 2022–2025, actas de ejercicios, evaluación de resultados, lecciones aprendidas, responsables, tiempos objetivo de recuperación, puntos objetivo de recuperación, dependencias críticas ni planes de acción derivados.

La evidencia de restauraciones puntuales es relevante, pero no equivale por sí sola a un plan de recuperación ante desastres formal, probado y mantenido. Un DRP debe permitir recuperar servicios críticos ante eventos mayores, no únicamente restaurar información en casos específicos. Por tanto, con la evidencia disponible no es posible concluir que la entidad cuente con capacidad integral, formalizada y validada de recuperación tecnológica frente a escenarios de desastre.

Criterio: Política GIT-PTI-POL-001 V.3 Manual de políticas de Seguridad de la Información; controles de continuidad, respaldos, restauración y recuperación ante desastres; requerimiento J2; riesgo GTI2.

Evidencia revisada: Estrategia DRP-ICA Preliminar.pdf; evidencias H2 de restauraciones y backup; evidencias relacionadas con monitoreo, disponibilidad y respaldo.

Riesgo asociado: GTI2 – posibilidad de afectación en la prestación de servicios por incumplir acuerdos de nivel de servicio tecnológicos debido a fallas de operación.

Efecto o riesgo: La ausencia de DRP final y probado puede generar exposición a indisponibilidad prolongada, pérdida de continuidad operativa, tiempos de recuperación no definidos y dificultad para restablecer servicios críticos ante incidentes mayores.

Recomendación 07
Formalizar, aprobar e implementar planes DRP para los servicios y sistemas críticos de la entidad, priorizando aquellos con alto impacto en la operación institucional. Los planes deberían incluir escenarios de desastre, responsables, contactos, dependencias, infraestructura requerida, RTO, RPO, procedimientos de recuperación, criterios de activación, retorno a la normalidad, pruebas periódicas, resultados, lecciones aprendidas y acciones de mejora.

Se recomienda ejecutar pruebas periódicas documentadas de continuidad y recuperación, conservar actas de resultados, registrar desviaciones y hacer seguimiento a los planes de acción derivados.

Observación 08. Seguimiento contractual de controles de seguridad y ANS/SLA no evidenciado de forma integral..

En los componentes **I1 – Proveedores y contratos**, **I2 – Soportes contractuales** y **K1 – Cumplimiento políticas**, se aportaron contratos, actas de inicio, estudios previos, acuerdos de confidencialidad y soportes contractuales relacionados con servicios tecnológicos, infraestructura, SOC y ciberseguridad. Estos documentos evidencian la existencia de soportes contractuales relevantes.

Sin embargo, no se evidenció una matriz consolidada que relacione los contratos TI/seguridad del periodo 2022–2025 con los servicios asociados, acceso a información o infraestructura, requisitos de seguridad, acuerdos de nivel de servicio, obligaciones de confidencialidad, tratamiento de datos, entregables, informes de supervisión, incidentes asociados, no conformidades, controles pactados y evidencia de cumplimiento.

La política exige que los riesgos de seguridad se identifiquen desde la etapa precontractual y que los contratos con proveedores incluyan requisitos de seguridad, confidencialidad, protección de datos, continuidad y niveles de servicio cuando aplique. Igualmente, se requiere seguimiento durante la ejecución contractual. La falta de consolidación dificulta verificar si los controles pactados se cumplen y si los proveedores mantienen los niveles de seguridad y disponibilidad requeridos.

Criterio: Política GIT-PTI-POL-001 V.3 Manual de políticas de Seguridad de la Información; controles de relación con proveedores; gestión contractual; acuerdos de nivel de servicio; requerimientos I1, I2 y K1.

Evidencia revisada: contratos GGC, actas de inicio, estudios previos SOC, acuerdo de confidencialidad, soportes contractuales y documentos asociados a servicios tecnológicos y ciberseguridad.

Riesgos asociados: GTI1 y GTI2.

Efecto o riesgo: La falta de trazabilidad contractual consolidada puede dificultar la verificación del cumplimiento de obligaciones de seguridad, confidencialidad, continuidad, disponibilidad y niveles de servicio, especialmente en servicios tercerizados con acceso a información o infraestructura institucional.

Recomendación 08
Consolidar una matriz de seguimiento contractual para contratos TI/seguridad del periodo evaluado y vigencias posteriores, que incluya número de contrato, objeto, proveedor, supervisor, vigencia, servicio asociado, acceso a información o infraestructura, requisitos de seguridad, obligaciones de confidencialidad, tratamiento de datos, SLA/ANS, entregables, informes de supervisión, incidentes, no conformidades y estado de cumplimiento.

Se recomienda que los supervisores contractuales incorporen dentro de sus informes evidencia específica sobre cumplimiento de obligaciones de seguridad de la información, niveles de servicio, continuidad, confidencialidad y gestión de incidentes cuando aplique.
Responsable sugerido: Jefatura OTI, supervisores contractuales y Equipo de Gestión Estratégica y Seguridad de Información TI.

Observación 09. Gestión de incidentes documentada mediante soportes por caso, sin un registro consolidado suficiente para el periodo evaluado.

En el componente **J1 – Gestión de incidentes**, se aportaron documentos relacionados con eventos o incidentes específicos, entre ellos situaciones asociadas a la página web institucional, Google Search Console, DNS y posible vulneración o hackeo de cuenta institucional de YouTube. También se allegaron formatos de incidentes de seguridad.

Estos soportes permiten evidenciar que algunos eventos fueron documentados y atendidos mediante comunicaciones, revisiones técnicas o registros específicos. Sin embargo, no se evidenció un registro consolidado de incidentes de seguridad para el periodo 2022–2025 que permita identificar, por cada evento: fecha, hora, sistema afectado, tipo de incidente, severidad, impacto, responsable, acciones de contención, acciones correctivas, fecha de cierre, lecciones aprendidas y controles ajustados.

La gestión por caso aporta trazabilidad puntual, pero no permite evaluar integralmente la gestión de incidentes. Sin un registro consolidado, se limita el análisis de recurrencia, tiempos de atención, tendencias, causas, impacto, efectividad de respuesta y cierre de acciones correctivas o preventivas.

Criterio: Política GIT-PTI-POL-001 V.3; controles de gestión de incidentes de seguridad; requerimiento J1; buenas prácticas de gestión de incidentes en el marco MSPI/SGSI.

Evidencia revisada: documentos de falla página web, Google Search Console, incidente página web, comunicaciones sobre DNS, posible vulneración de YouTube, revisión de cuenta YouTube, formatos de incidentes y soportes asociados.

Riesgos asociados: GOB2 y GTI2.

Efecto o riesgo: La ausencia de un registro consolidado dificulta el seguimiento institucional de incidentes, análisis de tendencias, medición de tiempos de respuesta, identificación de causas raíz y aplicación de acciones de mejora.

Recomendación 09
Formalizar y mantener actualizado un registro consolidado de incidentes de seguridad de la información para cada vigencia, incluyendo fecha y hora, sistema o servicio afectado, tipo de incidente, severidad, impacto, responsable, línea de tiempo, acciones de contención, análisis de causa, acciones correctivas, cierre, lecciones aprendidas y controles ajustados.

Se recomienda establecer reportes periódicos de incidentes para análisis de tendencias, seguimiento de recurrencias y toma de decisiones sobre controles preventivos, detectivos y correctivos.

Observación 10. Matriz de requisitos legales, contractuales y de privacidad no evidenciada de forma integral.

Para el componente **K1 – Cumplimiento políticas**, se aportaron soportes contractuales específicos, tales como estudio previo, contrato, acuerdo de confidencialidad y acta de inicio. Estos documentos son útiles para verificar obligaciones contractuales particulares relacionadas con seguridad y confidencialidad.

Sin embargo, no se evidenció una matriz integral de requisitos legales, contractuales y de privacidad aplicables a la OTI, al SGSI/MSPI y a los servicios tecnológicos bajo su gestión. Tampoco se evidenció una relación consolidada de sistemas, servicios o bases de datos que tratan datos personales, con sus responsables, obligaciones aplicables, controles técnicos, evidencias de cumplimiento y periodicidad de revisión.
La Política GIT-PTI-POL-001 V.3 contempla el cumplimiento de requisitos legales y contractuales, así como privacidad y protección de datos personales. En ese sentido, la entidad debe contar con mecanismos que permitan identificar qué obligaciones aplican, a qué sistemas o contratos corresponden, quién es responsable de su cumplimiento y qué evidencia se conserva para demostrarlo.

La falta de una matriz consolidada puede afectar la capacidad de la OTI para demostrar cumplimiento normativo de manera sistemática y trazable. También dificulta la identificación de obligaciones asociadas a proveedores, sistemas, servicios digitales, tratamiento de datos personales, confidencialidad, conservación de información y seguridad contractual.

Criterio: Política GIT-PTI-POL-001 V.3; MSPI; Resolución 500 de 2021; Resolución 2277 de 2025; requisitos legales, contractuales y de privacidad aplicables; requerimiento K1.

Evidencia revisada: ESTUDIO PREVIO SOC (2024).pdf; CONTRATO No. GGC-032-2024.pdf; Acuerdo confidencialidad ICA.pdf; ACTA DE INICIO GGC-032-2024.pdf.

Riesgo asociado: GOB2 – posibilidad de afectación reputacional por sanciones debido a omisión de normatividad aplicable en la implementación del SGSI/MSPI.

Efecto o riesgo: La ausencia de una matriz de cumplimiento legal, contractual y de privacidad limita la capacidad de seguimiento normativo, identificación de obligaciones aplicables y demostración de cumplimiento ante revisiones internas, externas o requerimientos de autoridades competentes.

Recomendación 10
Elaborar, actualizar y mantener una matriz integral de requisitos legales, contractuales y de privacidad aplicables a la OTI, al SGSI/MSPI y a los servicios tecnológicos bajo su gestión. Esta matriz debería incluir norma u obligación, descripción del requisito, sistema o proceso asociado, responsable, evidencia de cumplimiento, periodicidad de revisión, estado, fecha de actualización y acciones pendientes.

Se recomienda articular esta matriz con el inventario de activos de información, catálogo de sistemas y servicios, contratos tecnológicos, tratamiento de datos personales, acuerdos de confidencialidad, declaración de aplicabilidad y seguimiento al MSPI.

6. RIESGOS DE LA UNIDAD AUDITABLE:

El análisis de riesgos de la unidad auditable se desarrolló tomando como base los riesgos definidos en la planeación de auditoría, asociados al **Mapa de Riesgos Institucionales V1 2026**, y su relación con la evidencia aportada durante la fase de ejecución.

El propósito de este capítulo no es recalificar los riesgos institucionales ni sustituir la valoración realizada por el dueño del proceso. El análisis se orienta a verificar si los controles definidos frente a los riesgos auditables cuentan con evidencia suficiente, trazable y verificable que permita concluir preliminarmente sobre su operación, seguimiento y contribución a la mitigación del riesgo.

Para efectos del presente informe, se consideran los riesgos asociados a la unidad auditable identificados como **GTI1, GTI2, GOB1 y GOB2**, relacionados con adquisición de bienes y servicios tecnológicos, cumplimiento de acuerdos de nivel de servicio tecnológicos, alineación estratégica de tecnología y cumplimiento normativo en la implementación del SGSI/MSPI.

6.1 RIESGOS DEL MAPA DE RIESGOS INSTITUCIONAL ACTUAL.

Los riesgos incluidos en la planeación de auditoría fueron analizados a partir de: descripción del riesgo, zona inherente, causas, controles existentes, evidencia esperada, evidencia aportada y observaciones formuladas en el capítulo 5.4 del presente informe.
La trazabilidad entre riesgos, controles y observaciones permite identificar que varias situaciones observadas no constituyen riesgos nuevos, sino debilidades de evidencia, formalización, actualización, seguimiento o trazabilidad sobre controles ya relacionados con los riesgos institucionales existentes.

Riesgo GTI1. Posibilidad de afectación económica por inadecuada emisión de conceptos técnicos para la adquisición de bienes y servicios tecnológicos.

Descripción del riesgo
Este riesgo se refiere a la posibilidad de que la entidad tenga una afectación económica como consecuencia de conceptos técnicos inadecuados, insuficientes o no ajustados a los requisitos requeridos para adquirir bienes y servicios tecnológicos. El riesgo se encuentra asociado a decisiones de compra, contratación, adquisición o implementación de soluciones tecnológicas que podrían no responder a las necesidades institucionales, a los lineamientos técnicos, a los requisitos de seguridad o a los principios de eficiencia y control.

Zona inherente
Riesgo extremo.

Causas relevantes identificadas en la planeación
Las causas señaladas en la planeación se relacionan con presiones de terceros, desconocimiento de requisitos para adquirir bienes y servicios tecnológicos, recepción de dádivas o beneficios y omisión en los procedimientos de adquisición. Estas causas tienen incidencia directa en la calidad del concepto técnico, la transparencia del proceso y la pertinencia de las condiciones técnicas y de seguridad incorporadas en la contratación.

Control existente definido en la planeación
El control existente corresponde al visto bueno técnico del Jefe de la OTI, líder técnico y gerente de proyecto, frente al cumplimiento de requisitos técnicos antes del traslado a Gestión Contractual.

Este control busca asegurar que, antes de iniciar o trasladar un proceso contractual, los bienes o servicios tecnológicos cuenten con revisión técnica suficiente, validación de requisitos y concepto por parte de los responsables competentes.

Evidencia esperada:
Para verificar este riesgo y su control, se esperaría contar con evidencia como:

- Estudios previos.
- Conceptos técnicos.
- Requisitos técnicos de seguridad de la información.
- Vistos buenos del Jefe OTI, líder técnico y/o gerente de proyecto.
- Contratos, órdenes, actas y anexos técnicos.
- Evidencias de revisión de requisitos antes del traslado a Gestión Contractual.
- Obligaciones contractuales de seguridad, confidencialidad, disponibilidad, continuidad o soporte.
- Informes de supervisión contractual.
- Evidencia de cumplimiento de entregables técnicos y de seguridad.

Evidencia revisada
Durante la auditoría se revisaron soportes aportados en los componentes **I1 – Proveedores y contratos**, **I2 – Soportes contractuales** y **K1 – Cumplimiento políticas**, incluyendo contratos, estudios previos, actas de inicio, acuerdo de confidencialidad y documentos contractuales relacionados con servicios tecnológicos, infraestructura, SOC y ciberseguridad.

Análisis
La evidencia revisada permite identificar que existen soportes contractuales y documentos relacionados con servicios tecnológicos y de ciberseguridad. También se observan estudios previos, contratos, actas de inicio y acuerdos de confidencialidad, lo cual constituye una base documental relevante para verificar procesos de adquisición o contratación tecnológica.

No obstante, la evidencia no permite verificar de manera integral y consolidada que todos los contratos o procesos de adquisición tecnológica del periodo 2022–2025 cuenten con trazabilidad entre: necesidad técnica, análisis de seguridad, requisitos técnicos, aprobación del responsable competente, obligaciones contractuales, acuerdos de nivel de servicio, supervisión y cumplimiento de controles de seguridad.

La ausencia de una matriz consolidada de contratos TI/seguridad limita la verificación del control definido en la planeación, porque impide establecer, de forma rápida y completa, qué contratos tuvieron concepto técnico, qué requisitos de seguridad fueron incorporados, qué proveedor accedió a información o infraestructura, qué obligaciones fueron pactadas y cómo se realizó el seguimiento.

Resultado del riesgo
Evidencia parcial del control. Existen soportes contractuales relevantes, pero no se evidenció una consolidación integral que permita concluir sobre la operación sistemática del control para todo el periodo evaluado.

Observaciones relacionadas
Este riesgo se relaciona principalmente con:

- Observación 08. Seguimiento contractual de controles de seguridad y ANS/SLA no evidenciado de forma integral.
- Observación 10. Matriz de requisitos legales, contractuales y privacidad no evidenciada integralmente.

Conclusión sobre el riesgo GTI1
Con la evidencia revisada no se concluye materialización del riesgo; sin embargo, se identifica una debilidad de trazabilidad documental en el seguimiento de contratos y requisitos de seguridad. Esta situación puede afectar la capacidad de demostrar que los conceptos técnicos y los requisitos de seguridad fueron evaluados, aprobados y supervisados de forma homogénea durante el periodo auditado.

Riesgo GTI2. Posibilidad de afectación en la prestación de los servicios por incumplir los Acuerdos de Nivel de Servicio Tecnológicos debido a fallas de operación

Descripción del riesgo
Este riesgo se relaciona con la posibilidad de afectación en la prestación de servicios tecnológicos por fallas operativas, incumplimiento de acuerdos de nivel de servicio, indisponibilidad, falta de capacidad, debilidades de monitoreo, problemas de respaldo, incidentes técnicos, vulnerabilidades no tratadas o incumplimientos de proveedores.

Por su naturaleza, este riesgo se asocia directamente con la disponibilidad de sistemas, servicios digitales, infraestructura, redes, plataformas, bases de datos, mecanismos de respaldo y capacidades de recuperación.

Zona inherente
Riesgo extremo.

Causas relevantes identificadas en la planeación
Las causas definidas en la planeación incluyen fallas en bienes y servicios adquiridos, incumplimiento de proveedores, falta de herramientas de monitoreo, falta de personal capacitado y eventos ajenos a la operación ocasionados por terceros.
Estas causas se relacionan con los componentes técnicos evaluados en la auditoría: operación segura, respaldos, restauraciones, logs, monitoreo, vulnerabilidades, parches, continuidad, incidentes, contratos y niveles de servicio.

Controles existentes definidos en la planeación
La planeación definió dos controles principales:

1. Mantenimiento por proveedores con informe y aval del responsable de plataforma.
2. Verificación mensual de capacidad y disponibilidad de sistemas incluidos en los Acuerdos de Nivel de Servicio – ANS.

Estos controles buscan asegurar que los servicios tecnológicos cuenten con seguimiento técnico, mantenimiento adecuado, monitoreo de capacidad y disponibilidad, y validación por parte de responsables técnicos.

Evidencia esperada
Para verificar este riesgo y sus controles, se esperaría contar con evidencia como:

- Matriz de ANS/SLA tecnológicos.
- Informes mensuales de capacidad y disponibilidad.
- Reportes de monitoreo.
- Informes de mantenimiento de proveedores.
- Avales del responsable de plataforma.
- Registros de incidentes.
- Reportes de vulnerabilidades y planes de remediación.
- Evidencia de parches y protección contra malware.
- Logs de sistemas críticos.
- Pruebas de restauración.
- Planes DRP y resultados de pruebas.
- Informes de supervisión contractual.

Evidencia revisada
Se revisaron evidencias asociadas a:

- **H2 – Restauraciones y Backup.**
- **H3 – Gestión de Logs y trazabilidad.**
- **H5 – Gestión de vulnerabilidades.**
- **I1/I2 – Proveedores y contratos.**
- **J1 – Gestión de incidentes.**
- **J2 – Continuidad DRP.**
- Evidencias de monitoreo, disponibilidad y respaldo.
- Estrategia DRP preliminar.
- Contratos y soportes contractuales.
- Registros de incidentes específicos.

No se aportó evidencia para **H4 – Parches y protección Malware**.

Análisis
La evidencia revisada permite identificar que la OTI cuenta con soportes relacionados con restauraciones, respaldos, logs, análisis de vulnerabilidades, incidentes específicos y contratación de servicios tecnológicos. Estos elementos son relevantes para la gestión del riesgo GTI2, porque permiten observar actividades vinculadas con disponibilidad, recuperación, trazabilidad técnica y seguridad operativa.

No obstante, no se evidenció una matriz consolidada de ANS/SLA tecnológicos, ni reportes mensuales completos de capacidad y disponibilidad de los sistemas incluidos en dichos acuerdos. Tampoco se aportó evidencia de gestión de parches y protección malware, ni DRP final aprobado y probado para servicios críticos.

La existencia de restauraciones puntuales y soportes de logs demuestra actividades técnicas específicas, pero no permite concluir que exista un control integral, periódico y sostenido sobre la disponibilidad, capacidad, continuidad y recuperación de los servicios tecnológicos durante todo el periodo evaluado.

Resultado del riesgo
Evidencia parcial de los controles. Se identifican actividades técnicas relevantes, pero no se cuenta con evidencia suficiente para concluir sobre la operación completa de los controles definidos en la planeación.

Observaciones relacionadas
Este riesgo se relaciona principalmente con:

- Observación 05. No se aportó evidencia para verificar la gestión de parches y protección contra malware.
- Observación 06. Gestión de logs y trazabilidad con evidencia técnica parcial y sin esquema consolidado de control.
- Observación 07. Estrategia DRP y continuidad tecnológica en estado preliminar, sin evidencia suficiente de implementación y pruebas periódicas.
- Observación 08. Seguimiento contractual de controles de seguridad y ANS/SLA no evidenciado de forma integral.
- Observación 09. Gestión de incidentes con soportes por caso, sin registro consolidado suficiente para el periodo evaluado.

Conclusión preliminar sobre el riesgo GTI2
No se cuenta con evidencia suficiente para afirmar materialización del riesgo; sin embargo, los controles asociados presentan debilidades de evidencia y trazabilidad en ANS/SLA, parches, monitoreo consolidado, DRP y seguimiento contractual. Esto incrementa la exposición frente a indisponibilidad, fallas operativas, incidentes no gestionados integralmente y afectación en la prestación de servicios tecnológicos.

Riesgo GOB1. Posibilidad de afectación reputacional por diseñar e implementar planes estratégicos de tecnología no conformes con los lineamientos vigentes
Descripción del riesgo
Este riesgo se relaciona con la posibilidad de que la entidad diseñe o implemente planes estratégicos de tecnología sin alineación suficiente con los lineamientos institucionales, normativos, técnicos o de Gobierno Digital. La afectación se materializaría principalmente en términos reputacionales, por incumplimientos frente a lineamientos aplicables o por debilidades en la planificación estratégica de tecnología.

Zona inherente
Riesgo bajo.

Causas relevantes identificadas en la planeación
Las causas señaladas incluyen cambios de objetivos estratégicos sin participación de TI, desconocimiento de cambios normativos, falta de recurso humano competente, falta de recursos financieros y falta de gestión del cambio.

Estas causas pueden afectar la capacidad de la OTI para mantener actualizados sus planes, controles, proyectos, lineamientos y acciones frente a cambios normativos, tecnológicos o institucionales.

Control existente definido en la planeación
El control existente corresponde a la revisión anual del cumplimiento normativo de planes estratégicos y avance de implementación. Este control busca asegurar que los planes estratégicos de tecnología sean revisados frente a la normatividad aplicable y que exista seguimiento sobre el avance de implementación.

Evidencia esperada
Para verificar este riesgo y su control, se esperaría contar con evidencia como:

- Planes estratégicos de tecnología vigentes.
- Revisión anual de cumplimiento normativo.
- Seguimiento a avances de implementación.
- Actas de comités, mesas de trabajo o instancias de Gobierno Digital.
- Indicadores o reportes de avance.
- Evidencia de análisis de cambios normativos.
- Evidencia de alineación con MSPI y Gobierno Digital.
- Planes de acción o ajustes derivados de revisiones.

Evidencia revisada
Se revisaron documentos institucionales del SGSI/MSPI, documentos de proceso, documentación normativa, evidencias de divulgación, política de seguridad y privacidad, papeles de trabajo y soportes asociados a Gobierno Digital/MSPI. También se revisó información relacionada con la Resolución 500 de 2021 y la Resolución 2277 de 2025.

Análisis

La evidencia aportada permite identificar existencia de documentación institucional del SGSI/MSPI y de la política objeto de auditoría. Sin embargo, no se evidenció de manera consolidada una revisión anual del cumplimiento normativo de los planes estratégicos de tecnología, ni un seguimiento documentado del avance de implementación durante el periodo evaluado.

Tampoco se identificó una matriz o reporte que evidencie cómo se incorporaron los cambios normativos derivados de la actualización del MSPI mediante la Resolución 2277 de 2025 dentro de los planes, documentos, controles, declaración de aplicabilidad o acciones de implementación. La ausencia de esta trazabilidad limita la posibilidad de concluir que el control definido para el riesgo GOB1 haya operado de manera completa durante el periodo auditado.

Resultado del riesgo
Información pendiente de validación. Se identifican documentos institucionales y papeles de trabajo, pero no evidencia consolidada suficiente sobre revisión anual normativa de planes estratégicos y avance de implementación.

Observaciones relacionadas
Este riesgo se relaciona con las situaciones descritas en:

- Observación 02. Declaración de aplicabilidad y registro de excepciones sin evidencia suficiente de actualización frente al MSPI vigente.
- Observación 10. Matriz de requisitos legales, contractuales y privacidad no evidenciada integralmente.

Conclusión sobre el riesgo GOB1
No se concluye materialización del riesgo. Sin embargo, se requiere evidencia adicional que permita verificar la revisión anual de cumplimiento normativo de planes estratégicos de tecnología, el avance de implementación y la incorporación de cambios normativos, especialmente frente al MSPI actualizado.

Riesgo GOB2. Posibilidad de afectación reputacional por sanciones debido a la omisión de normatividad aplicable en la implementación del Sistema de Gestión de Seguridad de la Información

Descripción del riesgo
Este riesgo se refiere a la posibilidad de afectación reputacional para la entidad por omitir o aplicar de manera insuficiente la normatividad relacionada con la implementación del Sistema de Gestión de Seguridad de la Información – SGSI, el Modelo de Seguridad y Privacidad de la Información – MSPI, la Política de Seguridad y Privacidad de la Información y demás lineamientos aplicables.
Es el riesgo con mayor relación transversal frente a la auditoría, porque involucra gobierno, roles, controles, evidencias, actualización normativa, activos, accesos, incidentes, continuidad, proveedores, cumplimiento legal y privacidad.

Zona inherente
Riesgo extremo.

Causas relevantes identificadas en la planeación
Las causas identificadas incluyen desconocimiento normativo en seguridad de la información, falta de recursos financieros, falta de recursos humanos capacitados, falta de compromiso de la alta dirección, falta de compromiso de los responsables del sistema de gestión y falta de toma de conciencia de partes interesadas. Estas causas se relacionan con varios resultados de auditoría, especialmente aquellos asociados a formalización de roles, actualización de aplicabilidad, gestión de activos, accesos, logs, incidentes, privacidad y cumplimiento legal.

Controles existentes definidos en la planeación
La planeación definió como controles:

- Participación en mesas de trabajo de seguridad.
- Análisis e implementación de lineamientos impartidos.
- Revisión de cumplimiento de actividades en el marco de Gobierno Digital.
- Seguimiento mensual e implementación anual.

Estos controles buscan asegurar que la entidad analice, adopte e implemente los lineamientos aplicables de seguridad, privacidad y Gobierno Digital, y que exista seguimiento periódico a su cumplimiento.

Evidencia esperada
Para verificar este riesgo y sus controles, se esperaría contar con evidencia como:

- Matriz legal y normativa de seguridad y privacidad.
- Declaración de aplicabilidad actualizada.
- Registro de excepciones o aceptaciones de riesgo.
- Roles y responsabilidades formales.
- Evidencias de sensibilización.
- Matriz de activos de información actualizada.
- Matriz de riesgos y planes de tratamiento.
- Seguimiento mensual o periódico MSPI/SGSI.
- Informes de implementación anual.
- Actas de mesas de trabajo.
- Evidencias de cumplimiento Gobierno Digital.
- Registros de incidentes.
- Evidencia de privacidad y protección de datos personales.
- Auditorías o revisiones independientes.
- Planes de mejoramiento y seguimiento.

Evidencia revisada
Se revisaron evidencias de los componentes A1, A2, A3, C1, C2 parcial, D1, E1, E4, H3, J1, K1, documentos SGSI/MSPI, política auditada, documentos normativos y papeles de trabajo.

Análisis
La evidencia revisada permite identificar actividades de sensibilización, documentos institucionales del SGSI/MSPI, una declaración de aplicabilidad 2023, matriz de riesgos, plan de tratamiento 2024, soportes de incidentes específicos, algunos documentos de accesos y contratos. Sin embargo, no se aportó evidencia suficiente para concluir que los controles de este riesgo operen integralmente. Se identifican brechas en formalización de roles, actualización de declaración de aplicabilidad, registro de excepciones, matriz de activos actualizada, gestión integral de accesos, registro consolidado de incidentes, matriz legal/privacidad y seguimiento completo frente al MSPI actualizado.

La evidencia se presenta en varios casos de forma dispersa, por actividad o por caso, lo cual dificulta verificar seguimiento mensual, implementación anual y trazabilidad completa del SGSI/MSPI durante el periodo auditado.

Resultado del riesgo
Evidencia parcial de los controles. Existen soportes importantes, pero no se evidencia trazabilidad integral y actualizada del cumplimiento normativo SGSI/MSPI.

Observaciones relacionadas
Este riesgo se relaciona principalmente con:

- Observación 01. Formalización y trazabilidad de roles operativos de seguridad de la información.
- Observación 02. Declaración de aplicabilidad y registro de excepciones sin evidencia suficiente de actualización frente al MSPI vigente.
- Observación 03. Actualización anual de la matriz de activos de información no evidenciada para 2024 y 2025.
- Observación 04. Evidencia insuficiente de gestión integral de accesos e identidades.
- Observación 06. Gestión de logs y trazabilidad con evidencia técnica parcial y sin esquema consolidado de control.
- Observación 09. Gestión de incidentes con soportes por caso, sin registro consolidado suficiente para el periodo evaluado.
- Observación 10. Matriz de requisitos legales, contractuales y privacidad no evidenciada integralmente.

Conclusión sobre el riesgo GOB2
No se cuenta con evidencia suficiente para afirmar materialización del riesgo; sin embargo, el riesgo mantiene una exposición relevante debido a debilidades de actualización normativa, consolidación documental, trazabilidad de controles y seguimiento integral del SGSI/MSPI. La gestión de este riesgo requiere fortalecimiento prioritario, dado su carácter transversal frente a la política auditada.

Riesgo	Descripción resumida	Zona inherente	Control evaluado	Evidencia revisada	Resultado de la evaluación	Observaciones relacionadas
GTI1	Afectación económica por conceptos técnicos inadecuados para adquisición de bienes y servicios tecnológicos.	Extrema	Visto bueno técnico antes del traslado a Gestión Contractual.	Contratos, estudios previos, actas, soportes contractuales, acuerdo de confidencialidad.	Evidencia parcial. Falta consolidación contractual con trazabilidad de requisitos de seguridad, vistos buenos, ANS/SLA y seguimiento.	Observaciones 08 y 10.
GTI2	Afectación en la prestación de servicios por incumplir ANS tecnológicos debido a fallas de operación.	Extrema	Mantenimientos con informe/aval y verificación mensual de capacidad/disponibilidad.	Restauraciones, logs, vulnerabilidades, contratos, incidentes, DRP preliminar.	Evidencia parcial. No se evidenció matriz ANS/SLA, informes mensuales completos, parches/malware ni DRP final probado.	Observaciones 05, 06, 07, 08 y 09.

Riesgo	Descripción resumida	Zona inherente	Control evaluado	Evidencia revisada	Resultado de la evaluación	Observaciones relacionadas
GOB1	Afectación reputacional por planes estratégicos TI no conformes con lineamientos vigentes.	Baja	Revisión anual de cumplimiento normativo y avance de implementación.	Documentos SGSI/MSPI, normativa, papeles de trabajo, evidencias de cumplimiento.	No se aportó evidencia suficiente para verificar la revisión anual del cumplimiento normativo de los planes estratégicos y su avance de implementaciónn.	Observaciones 02 y 10.
GOB2	Afectación reputacional por omisión de normatividad aplicable en implementación SGSI/MSPI.	Extrema	Mesas de trabajo, análisis de lineamientos, revisión Gobierno Digital, seguimiento mensual e implementación anual.	A1, A2, A3, C1, C2 parcial, D1, E1/E4, H3, J1, K1 y documentos SGSI/MSPI.	Evidencia parcial. Debilidades de actualización, roles, activos, accesos, logs, incidentes, cumplimiento legal y privacidad.	Observaciones 01, 02, 03, 04, 06, 09 y 10.

6.2 MATERIALIZACIÓN DEL RIESGO.

Durante la auditoría se revisaron evidencias relacionadas con incidentes, fallas, vulnerabilidades, restauraciones, registros técnicos, contratos, continuidad y cumplimiento normativo. Sin embargo, con la información disponible al cierre de la auditoría no se cuenta con evidencia suficiente para afirmar la materialización formal de los riesgos GTI1, GTI2, GOB1 o GOB2 en los términos del Mapa de Riesgos Institucional.

Lo anterior se sustenta en que, aunque se aportaron soportes de eventos específicos —por ejemplo, documentos relacionados con página web institucional, DNS, Google Search Console, posible vulneración de cuenta institucional de YouTube, restauraciones, análisis de vulnerabilidades y estrategia DRP preliminar— no se evidenció un análisis formal de materialización del riesgo que incluya, como mínimo:

- Identificación del riesgo institucional materializado.
- Fecha del evento.
- Descripción del evento.
- Causa raíz.
- Impacto económico, reputacional, operativo, legal o de seguridad.
- Control que falló o resultó insuficiente.
- Responsable del análisis.
- Acciones correctivas.
- Fecha de cierre.
- Actualización de la matriz de riesgos.
- Ajuste al plan de tratamiento.
- Reporte a instancias correspondientes, cuando aplique.

En consecuencia, los eventos y soportes revisados se consideran insumos relevantes para análisis de riesgo, pero no permiten declarar de manera concluyente la materialización de un riesgo institucional.

Análisis por riesgo frente a posible materialización

GTI1 – Adquisición de bienes y servicios tecnológicos
No se evidenció un evento documentado que demuestre afectación económica causada por emisión inadecuada de conceptos técnicos. Se revisaron contratos y soportes contractuales, pero no se aportó análisis formal de daño económico, incumplimiento técnico atribuible a concepto inadecuado, sanción, pérdida o afectación patrimonial asociada a este riesgo.
Por tanto, para GTI1 no se concluye materialización. La situación observada corresponde a debilidad de trazabilidad contractual y de seguimiento de requisitos de seguridad, no a materialización confirmada del riesgo.

GTI2 – Prestación de servicios y ANS tecnológicos
Se revisaron evidencias relacionadas con restauraciones, logs, vulnerabilidades, incidentes, continuidad y contratos. También se identificaron soportes sobre eventos tecnológicos y afectaciones específicas. Sin embargo, no se aportó un análisis formal que relacione dichos

eventos con incumplimiento de ANS tecnológicos, indisponibilidad medida, impacto operativo, incumplimiento contractual, afectación institucional o falla de control.
Por tanto, no se concluye materialización de GTI2. No obstante, este riesgo presenta señales de exposición por ausencia de evidencia en parches/protección malware, DRP preliminar, logs sin esquema consolidado y falta de matriz ANS/SLA.

GOB1 – Planes estratégicos TI no conformes
No se evidenció evento o reporte que demuestre afectación reputacional derivada de planes estratégicos de tecnología no conformes con lineamientos vigentes. La auditoría identificó necesidad de mayor trazabilidad sobre revisión normativa y actualización frente al MSPI vigente, pero no una materialización formal de este riesgo.
Por tanto, GOB1 queda sin materialización evidenciada en esta etapa.

GOB2 – Omisión normativa en implementación SGSI/MSPI
La auditoría identificó debilidades de evidencia en actualización normativa, declaración de aplicabilidad, matriz legal, gestión de activos, accesos, logs e incidentes. No obstante, no se aportó soporte que demuestre sanción, requerimiento de autoridad, incumplimiento declarado, pérdida reputacional formal o evento institucional que permita afirmar materialización del riesgo.
Por tanto, no se concluye materialización de GOB2. Las observaciones formuladas constituyen advertencias preventivas y oportunidades de fortalecimiento del control, antes de que una posible omisión normativa derive en afectación material.

Conclusión sobre materialización
Con base en la evidencia revisada, **no se declara materialización de riesgos institucionales**. Sin embargo, se identifican condiciones de control que podrían aumentar la exposición frente a GTI1, GTI2, GOB1 y GOB2 si no se fortalecen la trazabilidad, actualización, seguimiento y cierre de controles.

Durante la etapa de discusión la OTI no aportó análisis formales de materialización, informes de afectación, actualizaciones de la matriz de riesgos ni soportes adicionales asociados a los eventos revisados. En consecuencia, se mantiene la conclusión de que no existe evidencia suficiente para declarar la materialización formal de los riesgos GTI1, GTI2, GOB1 o GOB2.

6.3. RIESGOS IDENTIFICADOS POR LA OFICINA DE CONTROL INTERNO QUE NO SE ENCUENTRAN EN EL MAPA DE RIESGOS INSTITUCIONAL.

La Oficina de Control Interno no formula un riesgo nuevo independiente al Mapa de Riesgos Institucional para la unidad auditable. Las situaciones observadas durante la auditoría se encuentran razonablemente asociadas a los riesgos ya definidos en la planeación, principalmente GTI2 y GOB2, y en menor medida GTI1 y GOB1.

No obstante, la auditoría identificó factores de exposición que podrían ser considerados por la OTI y por los responsables de la gestión del riesgo en futuras actualizaciones de la matriz, ya sea como causas, subcausas, controles adicionales, indicadores de seguimiento o eventos de riesgo más específicos.

Estos factores no se formulan como riesgos nuevos en el presente informe definitivo, debido a que se encuentran razonablemente cubiertos por los riesgos GTI1, GTI2, GOB1 y GOB2. No obstante, deberán ser analizados por el dueño del riesgo como posibles causas, controles, indicadores o acciones de tratamiento.

Factores de exposición identificados para análisis del dueño del riesgo

Factor identificado por auditoría	Riesgo institucional relacionado	Razón del análisis	Tratamiento sugerido
Falta de matriz formal y trazable de roles y responsabilidades de seguridad de la información.	GOB2	Puede afectar la rendición de cuentas, seguimiento y operación de controles SGSI/MSPI.	Incorporarlo como causa o control de fortalecimiento dentro del riesgo GOB2.

Factor identificado por auditoría	Riesgo institucional relacionado	Razón del análisis	Tratamiento sugerido
Declaración de aplicabilidad y registro de excepciones sin evidencia suficiente de actualización frente al MSPI vigente.	GOB2 / GOB1	Puede generar desalineación frente a cambios normativos y controles aplicables.	Incorporar seguimiento a actualización normativa como control o indicador.
Matriz de activos de información sin evidencia de actualización anual 2024–2025.	GOB2 / GTI2	Puede afectar clasificación, protección, acceso, respaldo y continuidad de activos.	Incluir actualización anual como control medible.
Gestión de accesos sin evidencia integral de altas, bajas, modificaciones y recertificación.	GOB2 / GTI2	Puede generar accesos no autorizados, privilegios excesivos o cuentas no retiradas.	Incluir recertificación periódica como control clave.
Ausencia de evidencia de parches y protección malware.	GTI2 / GOB2	Aumenta exposición a vulnerabilidades conocidas, malware e indisponibilidad.	Incorporar indicador de cumplimiento de parches y cobertura antimalware/EDR.
Gestión de logs sin esquema consolidado de retención, protección y revisión.	GTI2 / GOB2	Puede limitar detección, respuesta, trazabilidad e investigación de incidentes.	Formalizar control de gestión de logs y alertamiento.
DRP preliminar sin evidencia de aprobación y pruebas periódicas.	GTI2	Puede afectar recuperación de servicios críticos ante eventos mayores.	Incorporar prueba periódica de DRP como control de continuidad.
Contratos TI/seguridad sin matriz consolidada de obligaciones, ANS/SLA y seguimiento.	GTI1 / GTI2	Puede dificultar supervisión de obligaciones de seguridad y disponibilidad.	Incluir seguimiento contractual de seguridad como control.
Incidentes documentados por caso, sin registro consolidado 2022–2025.	GOB2 / GTI2	Limita análisis de tendencias, recurrencia y lecciones aprendidas.	Implementar registro consolidado e indicadores de incidentes.
Falta de matriz integral de requisitos legales, contractuales y privacidad.	GOB2	Puede generar omisión de obligaciones legales o contractuales.	Incorporar matriz legal/privacidad como control del SGSI/MSPI.

Los factores anteriores se encuentran cubiertos parcialmente por los riesgos existentes, especialmente por el riesgo **GOB2**, relacionado con omisión normativa en la implementación del SGSI/MSPI, y por el riesgo **GTI2**, asociado a afectación en la prestación de servicios tecnológicos. Por tanto, no se recomienda crear de forma inmediata riesgos independientes sin que el dueño del proceso realice previamente un análisis de causas, controles existentes, nivel de exposición, materialidad y pertinencia.

Sin embargo, sí se recomienda que la OTI evalúe si dichos factores deben incorporarse en la matriz de riesgos como:

- nuevas causas;
- controles adicionales;
- indicadores de seguimiento;
- eventos de riesgo específicos;
- acciones de tratamiento;
- criterios de monitoreo;
- evidencias obligatorias para seguimiento.

7. SEGUIMIENTO A PLANES DE MEJORAMIENTO

Durante el desarrollo de la auditoría se revisaron los documentos y evidencias aportadas por la OTI en los componentes definidos para la fase de ejecución: Gobierno MSPI, inventario tecnológico, gestión de riesgos, activos de información, gestión de accesos, criptografía, seguridad física y ambiental, operación segura, proveedores y contratos, incidentes y continuidad, y cumplimiento legal o cumplimiento de políticas. Dentro de dicha información no se aportó una **Forma 4-510 – Plan de Mejoramiento de Auditoría Oficina Control Interno**, ni una **matriz de seguimiento a planes de mejoramiento vigente** asociada directamente a la unidad auditable o a observaciones previas relacionadas con la Política GIT-PTI-POL-001 V.3 Manual de políticas de Seguridad de la Información, el MSPI, el SGSI o controles de seguridad de la información.

En consecuencia, con base en la evidencia disponible, no fue posible efectuar un seguimiento específico al avance, cumplimiento, eficacia o cierre de acciones correctivas derivadas de auditorías anteriores sobre esta misma unidad auditable. Esta condición no permite concluir que no existan planes de mejoramiento vigentes; únicamente permite indicar que, dentro de los soportes allegados y revisados en el marco de esta auditoría, **no se aportó evidencia suficiente para verificar planes de mejoramiento previos asociados a la OTI y al objeto auditado**.

Es importante diferenciar el **Plan de Tratamiento de Riesgos** aportado como papel de trabajo del **Plan de Mejoramiento de Auditoría**. El primero corresponde a un instrumento de gestión de riesgos, orientado al tratamiento de riesgos identificados y a sus controles; el segundo corresponde a la herramienta mediante la cual se consolidan las acciones de mejora derivadas de observaciones o hallazgos de auditoría. El procedimiento CIG-OCI-P-002 define el plan de mejoramiento como la herramienta que consolida y evidencia hallazgos, oportunidades de mejora, seguimiento a desviaciones de la gestión y acciones de mejoramiento continuo emprendidas por la entidad.

Por lo anterior, para efectos de este informe preliminar, el seguimiento a planes de mejoramiento se registra de la siguiente manera:

Aspecto revisado	Resultado del seguimiento
Existencia de plan de mejoramiento vigente asociado a la unidad auditable	No se aportó evidencia suficiente dentro de los soportes revisados.
Evidencia de Forma 4-510 asociada a auditorías anteriores sobre OTI / SGSI / MSPI / Política GIT-PTI-POL-001 V.3	No se aportó evidencia.
Matriz de seguimiento OCI con acciones abiertas o cerradas vinculadas a la unidad auditable	No se aportó evidencia.
Evidencia de avance, cumplimiento o cierre de acciones correctivas previas	No se aportó evidencia suficiente.
Posibilidad de verificar reincidencia de observaciones frente a auditorías anteriores	No fue posible verificar la reiteración de observaciones, debido a que no se aportó un plan de mejoramiento previo ni una matriz de seguimiento asociada al objeto auditado.

Con base en lo anterior, no se formularon observaciones reiterativas en este informe preliminar, debido a que no se contó con soporte documental suficiente para comparar las situaciones identificadas en esta auditoría con planes de mejoramiento anteriores. Durante la etapa de discusión no se aportaron planes de mejoramiento anteriores ni matrices de seguimiento adicionales. En consecuencia, no fue posible efectuar comparación para determinar reiteración de las observaciones formuladas.

Al quedar en firme y oficializarse el presente informe, las diez observaciones y sus recomendaciones deberán trasladarse a la Forma 4-510 – Plan de Mejoramiento de Auditoría Oficina Control Interno, conforme al procedimiento institucional. El CIG-OCI-P-002 prevé que, después de la comunicación de resultados, el equipo auditor diligencie en la Forma 4-510 los campos correspondientes a observaciones, recomendaciones, responsables, área auditada y vigencia, y que el área responsable formule las causas probables, acciones de mejora, responsables y fechas de inicio y terminación.

En ese sentido, las observaciones definitivas de esta auditoría deberán ser analizadas por la OTI para identificar sus causas y formular las correspondientes acciones correctivas o de mejora. Estas acciones deberán ser específicas, verificables, medibles y trazables frente a cada observación, evitando formular compromisos genéricos que no permitan evaluar su cumplimiento posterior.

Para la suscripción del plan de mejoramiento derivado de esta auditoría, se recomienda que la OTI tenga en cuenta, como mínimo, los siguientes elementos: causa raíz de cada observación, acción correctiva o preventiva, responsable funcional y operativo, fecha de inicio, fecha de terminación, producto o evidencia esperada, indicador de cumplimiento, riesgo asociado, control que se fortalece y mecanismo de seguimiento. El procedimiento también prevé que la Oficina de Control Interno analice la Forma 4-510 propuesta por las áreas responsables y registre recomendaciones de ajuste cuando aplique, antes de la oficialización del plan de mejoramiento.

8. RECOMENDACIONES GENERALES Y CONCLUSIONES

8.1 Recomendaciones generales

Primera. Fortalecer la gobernanza del SGSI/MSPI y la trazabilidad de responsabilidades. Se recomienda formalizar y mantener actualizada una matriz integral de roles y responsabilidades de seguridad de la información, en la cual se identifique de manera clara quién ejecuta, aprueba, revisa, monitorea y reporta cada control relevante de la Política GIT-PTI-POL-001 V.3. Esta matriz debe cubrir, entre otros aspectos, gestión de activos, accesos, cuentas privilegiadas, vulnerabilidades, respaldos, logs, incidentes, continuidad, proveedores, cumplimiento normativo y privacidad. La definición de responsabilidades no debe limitarse a grupos funcionales; debe permitir establecer responsables, suplencias, autoridad, periodicidad, evidencia esperada y ruta de escalamiento.

Segunda. Actualizar la declaración de aplicabilidad y el registro de excepciones frente al MSPI vigente. Se recomienda actualizar la declaración de aplicabilidad del SGSI/MSPI, incorporando la trazabilidad frente al marco vigente del Modelo de Seguridad y Privacidad de la Información, la Resolución 2277 de 2025 y los controles aplicables de la NTC/ISO 27001. Esta actualización debe permitir identificar controles aplicables, controles no aplicables, justificación de exclusiones, controles compensatorios, riesgos aceptados, responsables, aprobaciones y estado de implementación. De manera complementaria, se debe mantener un registro formal de excepciones, dispensas o aceptaciones de riesgo frente a la política de seguridad y privacidad.

Tercera. Consolidar la gestión de activos de información y activos tecnológicos. Se recomienda actualizar la matriz de activos de información para las vigencias pendientes y para la vigencia actual, asegurando que contenga propietario, custodio, clasificación, criticidad, ubicación, sistema asociado, tratamiento de datos personales si aplica, controles asociados y fecha de actualización. La matriz de activos de información debe articularse con los catálogos de sistemas, servicios, inventarios tecnológicos, inventario de servidores, certificados, respaldos, continuidad, vulnerabilidades y controles de acceso. Esto permitiría una gestión más coherente del riesgo y una aplicación más precisa de controles de confidencialidad, integridad, disponibilidad y privacidad.

Cuarta. Implementar trazabilidad integral sobre accesos e identidades. Se recomienda consolidar un modelo de gestión de accesos que cubra altas, bajas, modificaciones, accesos remotos, cuentas privilegiadas, cuentas de servicio, accesos de terceros, VPN y accesos a sistemas críticos. La evidencia debe permitir verificar solicitud, justificación, aprobación, implementación, cierre, retiro y revisión periódica. Adicionalmente, se recomienda realizar recertificaciones periódicas de accesos, especialmente sobre sistemas críticos, infraestructura, ambientes productivos y cuentas privilegiadas.

Quinta. Documentar y monitorear formalmente la gestión de parches, antimalware y vulnerabilidades. Se recomienda implementar reportes periódicos de cumplimiento de parches y protección contra malware o EDR, diferenciando servidores, estaciones, sistemas críticos y componentes administrados por terceros. Estos reportes deben vincularse con los resultados de análisis de vulnerabilidades, planes de remediación, responsables, fechas de cierre, excepciones y aceptación formal de riesgos cuando corresponda. La ausencia de evidencia en este componente limita la posibilidad de demostrar la operación efectiva de controles preventivos frente a amenazas técnicas.

Sexta. Formalizar el esquema institucional de gestión de logs y trazabilidad técnica. Se recomienda definir un procedimiento o matriz de gestión de logs que identifique fuentes de registro, sistemas cubiertos, eventos mínimos, responsables, ubicación de almacenamiento, tiempos de retención, controles de acceso, protección contra alteración, sincronización horaria, revisión periódica, alertas y escalamiento. La existencia de archivos de logs es un insumo útil, pero no demuestra por sí sola la efectividad del control si no existe una estructura formal de administración, revisión y protección de dichos registros.

Séptima. Formalizar, aprobar y probar el DRP para servicios críticos. Se recomienda culminar la formalización del Plan de Recuperación ante Desastres – DRP para servicios y

sistemas críticos de la entidad, incluyendo responsables, escenarios, dependencias, prioridades, RTO, RPO, procedimientos de recuperación, criterios de activación, retorno a la normalidad y pruebas periódicas. Las restauraciones puntuales son relevantes, pero deben integrarse a una estrategia de continuidad y recuperación aprobada, probada y mantenida.

Octava. Consolidar el seguimiento contractual de obligaciones de seguridad y ANS/SLA. Se recomienda implementar una matriz de seguimiento contractual para contratos de tecnología, seguridad, infraestructura, SOC, servicios tercerizados o proveedores con acceso a información o infraestructura. Esta matriz debe relacionar objeto, proveedor, supervisor, vigencia, servicio asociado, acceso a información, requisitos de seguridad, obligaciones de confidencialidad, tratamiento de datos, ANS/SLA, informes de supervisión, incidentes, entregables, no conformidades y estado de cumplimiento. La gestión contractual debe permitir demostrar no solo la existencia del contrato, sino el seguimiento efectivo de los controles pactados.

Novena. Consolidar la gestión institucional de incidentes de seguridad. Se recomienda mantener un registro consolidado de incidentes de seguridad para cada vigencia, que incluya fecha, sistema afectado, tipo de incidente, severidad, impacto, responsable, acciones de contención, acciones correctivas, fecha de cierre, lecciones aprendidas y controles ajustados. Los soportes por caso son útiles, pero deben integrarse en un registro institucional que permita análisis de tendencias, recurrencia, causas, tiempos de respuesta y efectividad de las acciones implementadas.

Décima. Elaborar o actualizar la matriz legal, contractual y de privacidad aplicable a OTI/SGSI/MSPI. Se recomienda estructurar una matriz integral de requisitos legales, contractuales y de privacidad aplicables a los servicios tecnológicos, sistemas de información, proveedores, activos de información, tratamiento de datos personales, contratos y controles de seguridad bajo responsabilidad de la OTI. Esta matriz debe incluir norma u obligación, descripción del requisito, responsable, evidencia de cumplimiento, periodicidad de revisión, estado y acciones pendientes.

Décima primera. Fortalecer la evidencia de seguimiento y mejora continua. Se recomienda que los controles del SGSI/MSPI cuenten con evidencia periódica de ejecución, revisión, seguimiento, cierre y mejora. En varios componentes la auditoría identificó soportes individuales o por caso, pero no consolidaciones que permitan demostrar operación sostenida durante el periodo evaluado. Para mejorar la trazabilidad, cada control debería contar con un expediente o repositorio estructurado que relacione criterio, responsable, evidencia, periodicidad, resultado y acciones de mejora.

Décima segunda. Formular un plan de mejoramiento específico, medible y verificable. Concluida la etapa de discusión y emitido el presente informe definitivo, la OTI deberá formular el Plan de Mejoramiento en la Forma 4-510, incorporando acciones concretas para cada una de las diez observaciones. Para cada acción se debe definir responsable, fecha de inicio, fecha de terminación, producto verificable, indicador de cumplimiento y mecanismo de seguimiento. El procedimiento CIG-OCI-P-002 prevé la formulación, análisis, ajuste, oficialización y posterior incorporación del plan de mejoramiento a la matriz consolidada de seguimiento.

8.2 Conclusiones

Con base en la evidencia revisada, se identifican avances y soportes relevantes por parte de la Oficina de Tecnologías de la Información en materia de sensibilización, inventarios tecnológicos, gestión de cambios, cuentas privilegiadas, restauraciones, logs, análisis de vulnerabilidades, contratación de servicios tecnológicos, soportes de incidentes específicos y estrategia preliminar de continuidad. Estos elementos constituyen una base documental y técnica útil para la implementación de la Política GIT-PTI-POL-001 V.3.
No obstante, a evidencia disponible no permite concluir que la Política GIT-PTI-POL-001 V.3 Manual de políticas de Seguridad de la Información se encuentre implementada de manera integral, trazable y sostenida en todos los componentes evaluados durante el periodo 2022–2025. La condición transversal observada es que existen soportes por actividad, archivo o caso específico, pero no siempre se cuenta con consolidación por control, vigencia, responsable, periodicidad, resultado, seguimiento y cierre.

El objetivo de evaluar la aplicación, implementación y cumplimiento de la política fue desarrollado mediante revisión documental y análisis de evidencias frente al MSPI, la Resolución 500 de 2021, la Resolución 2277 de 2025, la referencia aplicable de NTC/ISO 27001 y los documentos institucionales suministrados. El resultado de la auditoría evidencia aplicación parcial de controles y prácticas de seguridad de la información, así como brechas de formalización, actualización normativa, trazabilidad, consolidación y seguimiento.

Los riesgos definidos en la planeación —GTI1, GTI2, GOB1 y GOB2— resultan pertinentes frente al objeto auditado. No se contó con evidencia suficiente para declarar la materialización formal de dichos riesgos; sin embargo, las observaciones identificadas muestran factores de exposición que pueden incrementar su probabilidad o impacto si no se fortalecen los controles. Las mayores exposiciones identificadas se concentran en el riesgo **GTI2**, por su relación con disponibilidad, operación, continuidad, ANS/SLA, vulnerabilidades, parches, logs e incidentes, y en el riesgo **GOB2**, por su relación con cumplimiento normativo, SGSI/MSPI, roles, aplicabilidad, activos, accesos, privacidad y gestión de incidentes.

La auditoría permitió verificar la existencia de múltiples soportes documentales y técnicos; sin embargo, en varios casos la evidencia no fue suficiente para demostrar la operación integral de los controles durante todo el periodo auditado. Las principales limitaciones corresponden a ausencia o insuficiencia de evidencia en gestión integral de accesos, parches y protección malware, seguimiento completo de planes de tratamiento, matriz legal y privacidad, DRP probado, consolidación de ANS/SLA y registro consolidado de incidentes.

Con la evidencia disponible no es procedente afirmar cumplimiento integral del MSPI actualizado ni de los controles aplicables de NTC/ISO 27001. Sí se identifican avances en dominios específicos, pero se requiere fortalecer la actualización de la declaración de aplicabilidad, la trazabilidad de controles, la evidencia de seguimiento, la formalización de roles, la actualización de activos, el registro de excepciones y la gestión sistemática de cumplimiento legal, contractual y privacidad.

No se aportó evidencia suficiente de planes de mejoramiento vigentes asociados a la unidad auditable o al objeto de auditoría, por lo cual no fue posible verificar avance, cierre o eficacia de acciones correctivas previas. Las diez observaciones contenidas en el presente informe definitivo deberán incorporarse en la Forma 4-510, conforme al procedimiento institucional, y serán objeto de seguimiento por la Oficina de Control Interno.

El presente informe tiene carácter definitivo. El Informe Preliminar fue comunicado a la Oficina de Tecnologías de la Información – OTI para su revisión y discusión dentro del término establecido en el Procedimiento CIG-OCI-P-002. La OTI no presentó observaciones ni aportó evidencia adicional que modificara los resultados comunicados. En consecuencia, las diez observaciones y sus correspondientes recomendaciones se mantienen en los términos expuestos y constituyen la base para la formulación del Plan de Mejoramiento en la Forma 4-510. El informe se emite para su aprobación, oficialización, comunicación de resultados y seguimiento, con el propósito de fortalecer el control interno, la gestión de riesgos, la seguridad y privacidad de la información y la mejora continua del SGSI/MSPI institucional.

FIRMA DE APROBACIÓN	NOMBRE Y FIRMA DEL(LOS) AUDITOR(ES)	FECHA DE APROBACIÓN
Sandra Piedad Riaño Bustamante **Jefe Oficina Control Interno**	**Carlos Andrés Gómez Gómez**	**30/07/2026**