Fecha de Emisión del Informe	Día	3	Mes	08	Año	2026

Número de Informe:	1/2
Nombre:	Informe de seguimiento a la verificación del desarrollo y mantenimiento de los controles de TI – Seguridad de la Información
Objetivo:	Verificar que los controles de Tecnologías de la Información (TI) relacionados con la Seguridad de la Información se encuentren implementados, operando de manera adecuada y manteniéndose de forma continua, con el objetivo de proteger la información y los servicios tecnológicos de la Entidad frente a riesgos que puedan afectar su confidencialidad, integridad, disponibilidad y trazabilidad.
Alcance:	El presente seguimiento inicia con la solicitud y recopilación de la información relacionada con el desarrollo, implementación, operación y mantenimiento de los controles de Tecnologías de la Información (TI) asociados a la Seguridad de la Información. Posteriormente, comprende la revisión y evaluación de la documentación, registros y evidencias suministradas por las dependencias responsables, así como la verificación del cumplimiento de las actividades y controles implementados. El seguimiento concluye con la emisión del presente informe, en el que se presentan los resultados de la evaluación, el nivel de cumplimiento de los controles de TI en materia de Seguridad de la Información, y las oportunidades de mejora orientadas al fortalecimiento del Sistema de Gestión de Seguridad de la Información de la Entidad.
Periodicidad:	El informe se debe realizar dos (2) vez al año, con cortes a 31 de diciembre del 2025 y 30 de junio del 2026.

1. MARCO JURÍDICO.

El marco normativo está relacionado con los requisitos usados como referencia al presente informe al seguimiento a las políticas de gobierno digital:

- **Ley 87 del 1993,** Por la cual se establecen las normas para el ejercicio del Control Interno en las entidades y organismos del Estado.

- **Ley 1712 de 2014,** por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.

- **Ley 1581 de 2012 y el Decreto 1074 de 2015,** relacionados con la protección de datos personales y el régimen general de hábeas data.

- **Decreto 1078 de 2015**, Decreto Único Reglamentario del Sector Tecnologías de la Información y las Comunicaciones, y sus modificaciones, que establece los lineamientos para la gestión de las Tecnologías de la Información en las entidades públicas.

- **Modelo Integrado de Planeación y Gestión (MIPG)**, adoptado mediante el Decreto 1499 de 2017, particularmente en lo relacionado con la Política de Gobierno Digital, el fortalecimiento del control interno y la gestión institucional.

- **Política de Gobierno Digital**, expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), en lo referente a la implementación de capacidades para la seguridad digital y la protección de la información.

- **Modelo de Seguridad y Privacidad de la Información (MSPI)** del MinTIC, como referente para la implementación y fortalecimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas.

- **Resolución 500 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)**, **y su modificación con la resolución 2277 del 2025**, especialmente la **Resolución 746 de 2022**, por las cuales se establecen los lineamientos y estándares para la Estrategia de Seguridad Digital, se adopta el Modelo de Seguridad y Privacidad de la Información (MSPI) como habilitador de la Política de Gobierno Digital y se incorporan disposiciones adicionales para fortalecer la protección de los datos personales y la gestión de la seguridad digital en las entidades públicas.

- **Norma ISO/IEC 27001:2022**, como referente internacional para el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

Marco normativo del modelo integrado de planeación y gestión - MIPG

3ª. Dimensión: Gestión con valores para resultados

3.3.4 Política Gobierno Digital

La Política de Gobierno Digital es la política del Gobierno Nacional que propende por la transformación digital pública.

3.4.2 Política de Seguridad Digital

En materia de Seguridad Digital, el Documento CONPES 3854 de 2016 incorpora la Política Nacional de Seguridad Digital coordinada por la Presidencia de la República, para orientar y dar los lineamientos respectivos a las entidades.

7ª. Dimensión: Control Interno

7.1 Alcance de esta Dimensión

Control Interno

Lineamientos generales para la implementación

2. ALINEACIÓN CON EL MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓIN – MIPG.

Este informe de seguimiento al cumplimiento de las políticas de implementación de Gobierno Digital, esta alineado con las dimensiones 3° de gestión con valores para el resultado y 7° de control interno y contribuye a las directrices de la Política de Gestión y Desempeño Institucional, específicamente la política de Fortalecimiento organizacional y simplificación de procesos establecidos en el Modelo Integrado de Planeación y Gestión – MIPG adoptado por Unidad para las Victimas).

3. PROPÓSITO DEL INFORME.

El informe tiene como propósito presentar los resultados del seguimiento realizado a los controles de Tecnologías de la Información (TI) relacionados con la Seguridad de la Información, con el objetivo de dar a conocer el estado de su implementación, operación y mantenimiento, así como también el nivel de cumplimiento de las políticas, procedimientos, lineamientos internos y demás disposiciones aplicables.

Este informe está dirigido a la Dirección General y a los integrantes del Comité Institucional de Control Interno. Asimismo, puede ser de interés para los líderes de procesos y dependencias, los servidores públicos en general, y cualquier persona que lo consulte con fines académicos, de control social o por cualquier otra motivación legal.

De igual manera, el informe busca identificar fortalezas, riesgos y oportunidades de mejora en la gestión de los controles de seguridad de la información, proporcionando a la Alta Dirección y a los responsables del proceso información objetiva y oportuna que facilite la toma de decisiones, contribuya al fortalecimiento del Sistema de Gestión de Seguridad de la Información (SGSI) y promueva la mejora continua de los mecanismos implementados para proteger los activos de información y los servicios tecnológicos de la Entidad.

4. CONTEXTO DEL INFORME.

La transformación digital ha incrementado significativamente la dependencia de las entidades públicas de las Tecnologías de la Información (TI) para soportar sus procesos estratégicos, misionales, de apoyo y de evaluación. En este escenario, la información se consolida como uno de los activos más valiosos de la Entidad, cuya protección resulta indispensable para garantizar la continuidad de la operación, la prestación de los servicios, el cumplimiento de los objetivos institucionales y la confianza de los ciudadanos.

En este contexto, la Seguridad de la Información trasciende a la implementación de herramientas tecnológicas y se entiende como un proceso integral que combina personas, procesos y tecnología para gestionar los riesgos que puedan afectar la confidencialidad, integridad, disponibilidad y trazabilidad de la información. Para ello, es necesario que los controles de TI no solo se encuentren implementados, sino que operen de manera consistente, sean objeto de seguimiento permanente y evolucionen conforme cambian las amenazas, las vulnerabilidades y las necesidades del negocio.

Bajo este enfoque, la Oficina de Control Interno realizó el presente seguimiento con el propósito de evaluar el estado de los controles de TI asociados a la Seguridad de la Información, verificando su diseño, implementación, operación y mantenimiento. La evaluación permitió determinar si los controles implementados son acordes con los riesgos tecnológicos identificados, si contribuyen al cumplimiento de la normativa vigente y de las políticas institucionales, y si proporcionan un nivel de protección adecuado para los activos de información que soportan la operación de la Entidad.

Este ejercicio de seguimiento también constituye un mecanismo preventivo que aporta valor a la gestión institucional, al generar una visión objetiva sobre la efectividad de los controles implementados, identificar oportunidades de fortalecimiento y promover la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI). De esta manera, se contribuye a incrementar la resiliencia tecnológica de la Entidad, fortalecer su capacidad para prevenir, detectar y responder oportunamente a incidentes de seguridad, y apoyar el cumplimiento de los

principios de eficiencia, transparencia, disponibilidad y confiabilidad que orientan la administración pública.

5. RESULTADOS DEL ANÁLISIS Y VALIDACIÓN DE EVIDENCIAS.

La Oficina de Control Interno mediante correo electrónico del viernes 03 de julio se solicitó al líder del proceso de la Oficina de Tecnologías de la Informacion la información relacionada con los avances y actividades realizadas sobre los controles implementados al cumplimiento normativo del Modelo de Seguridad y Privacidad de la Información, los riesgos asociados a seguridad de la información, continuidad operativa, gobierno digital, y gestión tecnológica.

Se recibió respuesta por parte de la Oficina de Tecnologías de la Información mediante correo electrónico del martes 14 de julio a las 20:55 p.m. de la siguiente manera:

> *"En atención a su comunicado, la Oficina de Tecnologías de la Información se permite dar respuesta a cada requerimiento, en los siguientes términos:*
>
> ***1.1 Política de Seguridad y Privacidad de la Información vigente***
>
> *La Política General y las Políticas Específicas de Seguridad de la Información vigentes se encuentran formalizadas mediante la Resolución 3157 del 10 de noviembre de 2021, "Por la cual se establecen los Objetivos, Política General y Políticas Específicas del Sistema de Gestión de Seguridad de la Información en la Unidad para la Atención y Reparación Integral a las Víctimas y se deroga la Resolución No. 740 del 11 de noviembre de 2014", publicada en el sitio web institucional: Resolución 3157 de 2021. De manera complementaria, la Política de Privacidad y Protección de Datos Personales se encuentra publicada en: Políticas de privacidad y protección de datos personales.*
>
> ***1.2 Acto administrativo de aprobación***
> *El acto administrativo de adopción de la política corresponde a la citada Resolución 3157 de 2021, expedida por la Dirección General de la Entidad. Adicionalmente, la Resolución 2728 de 2021, por la cual se adopta el Modelo Integrado de Planeación y Gestión – MIPG, asigna en su artículo 4 (numeral 11) el liderazgo de la política de Seguridad Digital a la Oficina de Tecnologías de la Información y a la Subdirección Red Nacional de Información, y en su artículo 21 el liderazgo del Sistema de Gestión de Seguridad de la Información a la Oficina de Tecnologías de la Información. Se adjuntan copias de ambos actos administrativos.*

1.3 Alcance del SGSI

El alcance del SGSI se encuentra definido en la Política General establecida en el artículo 2 de la Resolución 3157 de 2021 y ratificado en el numeral 2 del Plan Estratégico de Seguridad de la Información (PESI) v4 – 2026: cobija los procesos estratégicos, misionales, de apoyo y de evaluación de la Entidad, sus Direcciones Territoriales, así como funcionarios, contratistas y colaboradores contratados por terceros, en un escenario de corresponsabilidad, e incluye la implementación de controles relacionados con la confidencialidad, integridad, privacidad y disponibilidad de la información. Se adjunta en la carpeta compartida el documento PESI v4 de 2026.

1.4 Objetivos de Seguridad de la Información

Los objetivos del SGSI, establecidos en la Resolución 3157 de 2021 y retomados en el numeral 1.1 del PESI v4 – 2026, son: (A) proteger la información y sistemas de información, según estándares que salvaguarden la confidencialidad, integridad y disponibilidad de los activos de la Entidad; (B) implementar los controles de seguridad de la información para mitigar, reducir o eliminar la divulgación, pérdida o modificación no controlada de los activos; (C) realizar seguimiento a los eventos e incidentes de seguridad para obtener lecciones aprendidas y mejorar periódicamente el SGSI; (D) promover, mantener y establecer la cultura de seguridad de la información en la Entidad y sus partes interesadas; (E) incrementar la disponibilidad de servicios de TI y de operación a través del plan de continuidad de negocio; y (F) suministrar información confiable, íntegra, oportuna, accesible y de valor a la población víctima.

1.5 Manual del SGSI

La documentación del SGSI se administra en el marco del Sistema Integrado de Gestión (SIG) y está conformada, entre otros, por: la Resolución 3157 de 2021 (políticas); el Lineamiento de Tecnologías de la Información, versión 1 del 02/12/2024, código 140,06,04-12, el cual incluye el Dominio de Seguridad de la Información.

Como soporte se carga en la carpeta compartida el Manual del Sistema Integrado de Gestión donde se incluye el Sistema de Gestión de Seguridad de la Información.

1.6 Roles y responsabilidades

Los roles y responsabilidades en materia de seguridad de la información están definidos en:

(i) la Resolución 3157 de 2021, que establece el compromiso y la corresponsabilidad de la Dirección General y de los(as) Directores(as), Subdirectores(as) y Jefes de Oficina;

(ii) la Resolución 2728 de 2021 (artículos 4, 8 y 21), que asigna el liderazgo de la política de Seguridad Digital y del SGSI, y establece como función del Comité Institucional de Gestión y Desempeño "asegurar la implementación y desarrollo de las políticas de gestión y las directrices en materia de seguridad digital y de la información";

(iii) el numeral 8 del PESI v4 – 2026, que detalla las responsabilidades del Comité Institucional de Gestión y Desempeño (Alta Dirección), de las dependencias, de la Oficina de Tecnologías de la Información y de los funcionarios, contratistas y colaboradores.

(iv) El documento ESTRUCTURA ORGANIZACIONAL Y ROLES & RESPONSABILIDADES de la Oficina de Tecnologías de la Información, el cual se adjunta en la carpeta compartida, con tiene la estructura organizacional de la Oficina, así como los roles y responsabilidades por dominio, incluyendo Seguridad de la Información.

1.7 Organigrama funcional

La estructura de la Entidad está establecida en el Decreto 4802 de 2011. Al interior de la Oficina de Tecnologías de la Información, la operación se organiza por dominios funcionales (Infraestructura TI, Sistemas de Información, Servicios TI, Arquitectura Empresarial y Seguridad de la Información). En el documento ESTRUCTURA ORGANIZACIONAL Y ROLES & RESPONSABILIDADES se encuentra el organigrama funcional de la OTI con la conformación.

1.8 Designación del Oficial de Seguridad de la Información

En virtud del artículo 21 de la Resolución 2728 de 2021, el liderazgo del SGSI recae en la Oficina de Tecnologías de la Información, cuyo Jefe de Oficina ejerce el rol de responsable de seguridad de la información ante las instancias institucionales. Operativamente, el liderazgo técnico del SGSI se encuentra asignado al Profesional Especializado [Código 2028, Grado 24] responsable del dominio Seguridad de la Información de la OTI, conforme consta en el ítem "ACTUALIZACIÓN Y APROBACIÓN" del documento ESTRUCTURA ORGANIZACIONAL Y ROLES & RESPONSABILIDADES.

1.9 Actas del Comité de Seguridad de la Información de la vigencia auditada

De acuerdo con la Resolución 2728 de 2021, las funciones de instancia decisoria en materia de seguridad de la información son ejercidas por el Comité Institucional de Gestión y Desempeño (artículo 8, numeral 6). Se adjunta acta de la sesión del 29 de enero de 2026, en las que se trataron asuntos del SGSI, incluida la aprobación del PESI v4 – 2026, del Plan de Tratamiento de Riesgos 2026.

1.10 Indicadores del SGSI

Los indicadores del SGSI se encuentran definidos en el numeral 6.1.2 "Seguimiento, medición, análisis y evaluación" del PESI v4 – 2026 (Tabla 5), asociados a cada uno de los seis objetivos del sistema, con sus fórmulas y metas (índice de ciberseguridad de la Unidad, efectividad de controles del instrumento MSPI, gestión de vulnerabilidades, cultura de seguridad, continuidad y disponibilidad de la infraestructura, entre otros). Como referencia de resultados: la evaluación de efectividad de controles mediante el instrumento MSPI del MinTIC (base ISO/IEC 27001:2022) asciende a 75% a corte 2025; la calificación bajo el marco NIST CSF promedia 75,0; y la medición FURAG de la política de Seguridad Digital alcanzó 92,86 (2024). Se adjunta el reporte de medición de los indicadores del SGSI de la vigencia.

1.11 Informe de revisión por la Dirección

La revisión por la Dirección del SGSI se realizó en el marco del Sistema Integrado de Gestión en noviembre de 2023 como se observa en el archivo cargado en la compartida "1.11 InformeRevisionDireccion2023.pdf". Por otra parte, en los comités institucionales de gestión y desempeño se ha presentado el avance en cuanto a la implementación del Plan Estratégico de Seguridad de la Información (PESI).

2.1 Metodología de Gestión del Riesgo

La Entidad aplica la Metodología de Administración de Riesgos definida por la Oficina Asesora de Planeación, disponible en: Metodología de Administración de Riesgos. Conforme al numeral 5 del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2026, el marco de referencia incorpora las normas NTC-ISO/IEC 31000, NTC-ISO/IEC 27005 y NTC-ISO/IEC 27001.

2.2 Inventario de riesgos de Seguridad de la Información

Para la vigencia 2026 se identificaron y actualizaron 32 riesgos de seguridad de la información, con 81 controles existentes y 36 planes de acción asociados (Tabla 1 del Plan de Tratamiento de Riesgos 2026). Adicionalmente, para las Direcciones Territoriales se definen riesgos estandarizados de seguridad de la información, conforme a lo establecido en el PESI. Se adjunta archivo Excel con el mapa de riesgos institucional publicado en la página Web en la URL https://www.unidadvictimas.gov.co/documentos_bibliotec/mapa-de-riesgos-institucional-corrupcion-y-gestion-v2-2025/

2.3 Matriz de riesgos de Seguridad de la Información

Las matrices de riesgos de seguridad de la información por proceso fueron actualizadas para la vigencia 2026 en articulación con los Enlaces del Sistema Integrado de Gestión (SIG) y aprobadas por los líderes de los procesos. Se adjuntan las matrices en formato editable, con la redacción del riesgo, niveles de severidad inherente y residual, controles (con su tipificación: afectación, tipo, implementación, documentación, evidencia y frecuencia) y referencia a los controles del Anexo A de la norma ISO/IEC 27001:2022.

2.4 Planes de tratamiento

Los 36 planes de acción para el tratamiento de los riesgos se encuentran consolidados en el numeral 7 y siguientes del Plan de Tratamiento de Riesgos 2026, con fechas de ejecución comprendidas entre el 02/01/2026 y el 31/12/2026, evidencias esperadas y responsables (Enlaces SIG de los procesos o designados por los líderes de proceso). Se carga como soporte el plan de tratamiento de riesgos aprobado por el Comité Institucional de Gestión y Desempeño.

2.5 Evidencia del seguimiento efectuado

El seguimiento a los riesgos se realiza conforme al numeral 8.2 del Plan de Tratamiento de Riesgos 2026 (revisión, actualización y medición), en articulación con los Enlaces SIG, quienes cargan periódicamente las evidencias de la operación de los controles y de la ejecución de los planes de

acción. Se adjuntan los reportes de seguimiento con corte abril (Primer cuatrimestre) de 2026 para procesos y Direcciones Territoriales.

2.6 Riesgos aceptados por la Alta Dirección

Los riesgos con opción de tratamiento "Aceptar" corresponden a riesgos con nivel de severidad residual "Bajo", entre ellos: dos (2) riesgos del proceso de Gestión Administrativa, dos (2) del proceso de Evaluación Independiente, uno (1) del proceso de Control Interno Disciplinario y tres (3) riesgos asociados a la Subdirección Red Nacional de Información (proceso de Gestión de Información), según el detalle del Plan de Tratamiento de Riesgos 2026. La aceptación se surte en el marco de la aprobación del Plan por parte del Comité Institucional de Gestión y Desempeño y de la aprobación de las matrices por los líderes de proceso.

2.7 Riesgos asociados a servicios en la nube

Los riesgos asociados a los servicios en la nube se encuentran incorporados en la matriz del proceso de Gestión de Información, particularmente en los riesgos del Dominio de Infraestructura TI (disponibilidad de la información asociada a políticas de backups, gestión de identidades y control de acceso a repositorios como SharePoint y OneDrive) y en los controles transversales de los procesos relacionados con el uso de SharePoint/OneDrive como repositorios oficiales.

2.8 Riesgos asociados a terceros

Los riesgos relacionados con terceros están contemplados en:
(i) los riesgos y controles de los procesos que operan con operadores y proveedores.
(ii) la identificación de riegos con terceros, que involucra la etapa precontractual y contractual, por parte de la dependencia responsable de la estructuración del proceso en el marco del procedimiento de Planeación contractual y gestión contractual versión 12 del 25/09/2025 código 161,10,08-1 del proceso de Gestión Contractual. Ver procedimiento https://www.unidadvictimas.gov.co/wp-content/uploads/2018/10/Procedimiento-Planeacion-Contractual-Y-Gestion-V12.pdf,
actividad 25. Estructurar los estudios y documentos previos, análisis del sector, estudio de mercado, matriz de riesgos, Anexo técnico y/o Ficha Técnica demás documentos que requiera para modalidad de contratación.

3.1 Inventario de activos de información

El inventario de activos de información se actualiza anualmente en articulación con los Enlaces SIG de los procesos y Direcciones Territoriales, conforme a la macroactividad No. 1 del plan de trabajo del PESI v4 – 2026. Los instrumentos de gestión de la información pública derivados (Registro de Activos de Información, Índice de Información Clasificada y Reservada y Esquema de Publicación) son aprobados por el Comité Institucional de Gestión y Desempeño y publicados por la OTI en la sección de Transparencia del sitio web institucional, en cumplimiento de la Ley 1712 de 2014. Se carga en la carpeta compartida la matriz de activos de la vigencia 2025 con la correspondiente acta de aprobación del Comité Institucional de Gestión y Desempeño. Para la actual vigencia se adelanta

la actualización, revisión y consolidación previa a la presentación para aprobación por parte del mencionado comité.

3.2 Inventario de infraestructura tecnológica

El inventario de la infraestructura tecnológica se incluye en el inventario de activos de información. Se carga en la carpeta compartida el archivo "3.2. 15-09-2025 - Consolidado Activos 2025 - Filtro infraestructura TI.xlsx". Es importante indicar que, la Oficina de TI puede generar inventario detallado de equipos y de elementos de infraestructura cuando sea requerido. Por lo tanto, quedamos atentos a cualquier reporte detallado que sea requerido.

3.3 Inventario de servicios tecnológicos

La Entidad cuenta con el catálogo de servicios tecnológicos administrado a través de la Mesa de Servicios Tecnológicos de la OTI, que consolida los servicios de TI ofrecidos a los procesos y Direcciones Territoriales. Se adjunta el catálogo de servicios.

3.4 Metodología de clasificación e identificación de activos

La identificación y clasificación de activos se realiza conforme al procedimiento para la generación y/o actualización del inventario de activos de información del SIG, el cual establece los criterios de valoración por confidencialidad, integridad y disponibilidad, la identificación de activos críticos y la clasificación de la información conforme a la Ley 1712 de 2014 (pública, pública clasificada y pública reservada). Se carga en la carpeta compartida el procedimiento establecido, así como el instructivo y formato.

4.1 Política de autenticación

La política de control de acceso y autenticación hace parte de las Políticas Específicas establecidas en la Resolución 3157 de 2021 y del Dominio de Seguridad del Lineamiento de Tecnologías de la Información (código 140,06,04-12). Su implementación se fortaleció mediante el proyecto "Gestión de Identidades" (Fase 1, finalizado en 2025), que permitió desarrollar el módulo transversal de autenticación integrado con el Directorio Activo institucional, centralizando la autenticación para nuevos sistemas de información.

4.2 Política de contraseñas

Los lineamientos de contraseñas seguras hacen parte de las políticas específicas del SGSI y se materializan técnicamente mediante las políticas de grupo (GPO) del Directorio Activo (longitud mínima, complejidad, historial, vigencia y bloqueo por intentos fallidos).

4.3 Política de autenticación multifactor

Se tiene implementada la política MFA (Microsoft Entra ID) para Office 365 y para Azure. Se carga soporte en la carpeta compartida.

4.4 Relación de usuarios con privilegios administrativos

Se carga en la carpeta compartida:
(i)Captura de pantalla con usuarios administradores globales (Office)
(ii)Relación de usuarios administradores Azure

4.5 Evidencia de revisión periódica de usuarios
Se carga la relación de usuarios creados en Office 365 (de enero a junio de 2026). Asimismo, se carga la muestra de inactivación de cuentas de Office 365 en el marco de la gestión de cuentas.

4.6 Relación de cuentas genéricas y su justificación
Se remite la relación de cuentas genéricas de Office 365 las cuales fueron creados por demanda de manera documentada. Como muestra se carga la justificación documentada para la creación de la cuenta magdalenamediodt@unidadvictimas.gov.co.

4.7 Evidencia de implementación de MFA en plataformas institucionales
Se cargan capturas de pantalla de la configuración MFA de Microsoft Entra ID de Microsoft.
Adicionalmente, se carga documento con soportes de implementación del doble factor de autenticación en plataformas institucionales.

5.1 Procedimiento de gestión de vulnerabilidades
En el marco de la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) la Unidad para las Víctimas ha fortalecido el proceso de gestión de vulnerabilidades conforme al control A.8.8 – Gestión de Vulnerabilidades Técnicas del Anexo A de la ISO/IEC 27001:2022, estableciendo un proceso continuo para la identificación, evaluación, tratamiento y seguimiento de las vulnerabilidades que puedan afectar los activos de información institucionales.
La entidad gestiona las vulnerabilidades provenientes de múltiples fuentes de información. Entre ellas se encuentran los reportes emitidos por ColCERT del MinTIC, los cuales son analizados por el equipo de Seguridad de la Información para determinar su aplicabilidad e impacto sobre la infraestructura tecnológica de la Unidad. De manera complementaria, se realizan análisis periódicos de vulnerabilidades sobre la infraestructura interna, permitiendo identificar oportunamente debilidades de seguridad antes de que puedan ser explotadas.

5.2 Herramientas utilizadas
Microsoft Defender como fuente de amenazas internas y Nessus. Adicionalmente, se han realizado análisis de vulnerabilidades por parte del COLCERT del MinTIC con las siguientes herramientas:

- *SecurityScorecard*
- *Outpost24*

5.3 Últimos informes de escaneo
Últimamente se realizaron los siguientes análisis de vulnerabilidades en el año 2025

- *Servidores*
- *Endpoints (muestra)*

El ColCERT del MinTIC realizó al análisis de vulnerabilidades documentado en mayo de 2026

Debido a que estos informes contienen información sensible, se procede a cargar en la carpeta compartida los soportes anonimizados mediante la impresión parcial de cada documento.

5.4 Planes de remediación

Se cuenta con la matriz de seguimiento a las vulnerabilidades identificadas de los informes de escaneo, los cuales constituyen la línea base para la elaboración de planes de remediación, los cuales incluyen responsables, tiempos de implementación, validaciones posteriores y seguimiento hasta la eliminación o mitigación del riesgo. Este seguimiento ha permitido priorizar aquellas con mayor impacto sobre la confidencialidad, integridad y disponibilidad de la información.

Debido a que esta información es altamente sensible, respetuosamente se plantea que el seguimiento por parte de la Oficina de Control Interno para este ítem en particular se realice mediante sesión de trabajo presencial o virtual sin grabaciones. Por supuesto, frente a este ítem la Oficina de TI queda muy atenta a cualquier comunicado o solicitud en particular que realice la Oficina de Control Interno.

5.5 Estado de vulnerabilidades críticas

En el informe de vulnerabilidades realizado por el ColCert en mayo de 2026 se registraron cero (0) vulnerabilidades críticas en sistemas de información de la Entidad. No obstante, aún se cuentan con vulnerabilidades en entornos de pruebas para su cierre dado que estas afectan los modos de producción para su cierre total.

5.6 Evidencia del cierre de vulnerabilidades

La Oficina de TI cuenta con la matriz de gestión de vulnerabilidades para registro y seguimiento. Adicionalmente, la Unidad desarrolla y recibe informes de vulnerabilidades realizadas por el ColCert, cuyos hallazgos son incorporados al proceso de gestión de vulnerabilidades. Adicionalmente, cómo se indicó en el punto anterior, el informe de vulnerabilidades realizado por el ColCert en mayo de 2026 se registraron cero (0) vulnerabilidades críticas en sistemas de información de la Entidad.

Debido a que esta información es altamente sensible, respetuosamente se plantea que el seguimiento por parte de la Oficina de Control Interno para este ítem en particular se realice mediante sesión de trabajo presencial o virtual sin grabaciones. Por supuesto, frente a este ítem la Oficina de TI queda muy atenta a cualquier comunicado o solicitud en particular que realice la Oficina de Control Interno.

5.7 Informes de pruebas de penetración internas y externas

Debido a que estos informes contienen información sensible, se procede a cargar en la carpeta compartida los soportes anonimizados mediante la impresión parcial de cada uno de los siguientes documentos:

- Análisis de vulnerabilidades Servidores (interno)
- Análisis de vulnerabilidades de una muestra de Endpoints (interno)
- Análisis de vulnerabilidades. Realizado por el ColCert del MinTIC (Documento reciente)

5.8 Seguimiento a hallazgos derivados de dichas pruebas
El seguimiento se documenta en la matriz de gestión de vulnerabilidades.
Debido a que esta información es altamente sensible, respetuosamente se plantea que el seguimiento por parte de la Oficina de Control Interno para este ítem en particular se realice mediante sesión de trabajo presencial o virtual sin grabaciones. Por supuesto, frente a este ítem la Oficina de TI queda muy atenta a cualquier comunicado o solicitud en particular que realice la Oficina de Control Interno.

6.1 Inventario de servicios Cloud utilizados
Se carga inventario de servicios Cloud utilizados en la infraestructura tecnológica de la Unidad para las Víctimas.

6.2 Arquitectura Cloud
Se carga documento interno de trabajo con la arquitectura de servicios de nube.

6.3 Configuración de seguridad
Se carga reporte de la cobertura en Azure de la configuración de aseguramiento.

6.4 Evidencia de MFA
El acceso a Azure opera con las políticas de doble factor de autenticación mencionadas en el punto 4.3 Política de autenticación multifactor.

6.5 Políticas de acceso
Se carga captura de pantalla con las directivas (políticas) configuradas para Azure y Office 365, donde se incluye MFA y Bloqueo de autenticación en otros países, entre otras.

6.6 Reportes de auditoría
Los servicios de auditoría de Azure y de Office 365 están configurados por defecto. Se carga captura de pantalla con los servicios de auditoría configurados

6.7 Configuración de logs
Se carga capturas de pantalla del logAnalitics y datacolector rules. Adicionalmente, se carga el archivo 6.7 Logs 1 Group.png con las políticas de infraestructura de cómputo.

6.8 Configuración de respaldo
Se carga la política configurada para realización de copias de respaldo para servidores.

6.9 Configuración de cifrado
Se carga captura de pantalla con la configuración de cifrado de discos en Azure.

En los anteriores términos se da respuesta ítem por ítem a la solicitud de información formulada. La Oficina de Tecnologías de la Información se encuentra atenta a atender las mesas de trabajo, aclaraciones o requerimientos adicionales que el equipo auditor estime pertinentes durante el desarrollo de la evaluación, para lo cual se designa como enlace al Ingeniero Joaquín Rojas Palomino.

5.2 Análisis de la Informacion Oficina de Control Interno

Para la realización de este informe se realizó un análisis de los controles de seguridad de la información implementados por la Entidad, con el propósito de determinar su nivel de diseño, implementación y eficacia para proteger la confidencialidad, integridad y disponibilidad de la información institucional, así como verificar su alineación con los requisitos de la NTC ISO/IEC 27001:2022, el Modelo de Seguridad y Privacidad de la Información (MSPI) y la Resolución 2277 de 2025, que actualiza la Resolución 500 de 2021 en el marco de la Política de Gobierno Digital.

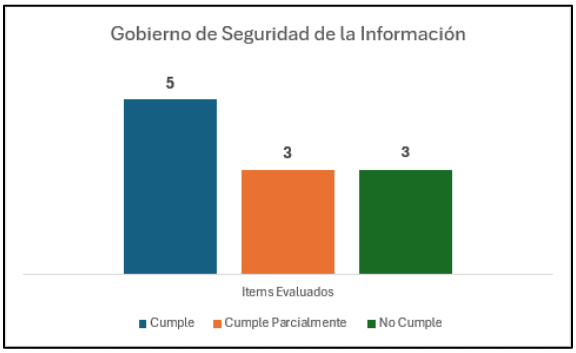
La evaluación se realizó sobre de los controles, que soportan el Sistema de Gestión de Seguridad de la Información (SGSI), verificando la existencia, formalización, implementación y efectividad de mecanismos orientados a gestionar los riesgos de seguridad de la información. En este contexto, se analizaron controles relacionados con el gobierno de la seguridad de la información, la política y los objetivos de seguridad, la definición de roles y responsabilidades, el alcance del SGSI, la gestión de activos de información, el control de accesos, la gestión de vulnerabilidades, la protección de la infraestructura tecnológica, la gestión de incidentes de seguridad, la continuidad del negocio, la gestión de terceros, la protección de la información y los mecanismos de seguimiento, monitoreo y mejora continua de los controles implementados.

El análisis se fundamentó en la revisión de la documentación suministrada, la validación de evidencias y la verificación del cumplimiento de los controles definidos por la Entidad frente a los requisitos normativos y las buenas prácticas internacionales. Como resultado, se identificaron fortalezas en la implementación de determinados controles de seguridad, así como oportunidades de mejora orientadas a incrementar la madurez del SGSI, fortalecer la gestión de riesgos y asegurar que los controles establecidos sean consistentes, medibles y efectivos para responder a las amenazas y vulnerabilidades que puedan afectar los activos de información institucionales.

Gobierno de Seguridad de la Información

La evaluación del componente Gobierno de Seguridad de la Información tuvo como propósito determinar si la Entidad cuenta con los elementos de direccionamiento estratégico, liderazgo, estructura organizacional y mecanismos de seguimiento necesarios para garantizar que la seguridad de la información se gestione de manera sistemática y conforme a los requisitos de la NTC ISO/IEC 27001:2022, el Modelo de Seguridad y Privacidad de la Información (MSPI) y la Resolución 2277 de 2025 en donde se tuvieron en cuenta 11 requerimientos.

Como resultado de la revisión, se evidenció que la Entidad ha establecido la mayoría de los controles de gobierno del SGSI; sin embargo, varios de ellos requieren actualización y fortalecimiento para mantener su alineación con el marco normativo vigente y con las mejores prácticas internacionales.



Fuente OTI – Análisis OCI

Requerimiento	Observación OCI
1. Política de Seguridad y Privacidad de la Información – Cumple parcialmente	El análisis permitió establecer que la Entidad cuenta con una Política General y Políticas Específicas de Seguridad de la Información, formalizadas mediante la Resolución 3157 del 2021, esto demuestra la existencia de un marco institucional para la gestión de la seguridad de la información. Sin embargo, dicho instrumento fue elaborado con los lineamientos de la ISO/IEC 27001:2013 asociada a la Resolución 500 de 2021, normativa que posteriormente fue actualizada mediante la Resolución 2277 de 2025, la cual incorpora nuevos lineamientos del Modelo de Seguridad y Privacidad de la Información alineados con la ISO/IEC 27001:2022. En consecuencia, la política vigente requiere ser revisada y actualizada para incorporar los nuevos principios, controles y enfoques de gestión del riesgo establecidos por la regulación vigente.

Requerimiento	Observación OCI
2. Acto administrativo de aprobación – Cumple	Se verificó la existencia del acto administrativo mediante el cual se adoptan las políticas de seguridad de la información, expedido por la Dirección General, así como la definición de responsabilidades institucionales mediante la Resolución 2728 de 2021. No obstante, se considera pertinente que, en futuras actualizaciones del marco documental, la Entidad incorpore expresamente las disposiciones de la Resolución 2277 de 2025, con el fin de mantener la trazabilidad normativa y asegurar la adopción de los nuevos lineamientos de seguridad digital.
3. Alcance del SGSI – No cumple	La evaluación determinó que la Entidad asocia el alcance del SGSI con el contenido del artículo 2 de la Resolución 3157 de 2021. Sin embargo, dicho artículo constituye una declaración de la política general y del compromiso institucional frente a la seguridad de la información, más no una definición formal del alcance del sistema. Desde la perspectiva de la ISO/IEC 27001:2022, el alcance debe establecer de forma precisa los procesos, sedes, activos de información, servicios tecnológicos, infraestructura, partes interesadas, terceros, interfaces y posibles exclusiones que hacen parte del SGSI. La ausencia de esta delimitación dificulta establecer los límites del sistema y evaluar adecuadamente la cobertura de los controles implementados.
4. Objetivos de Seguridad de la Información – Cumple parcialmente	Los objetivos definidos en la Resolución 3157 de 2021 y en el PESI se encuentran alineados con los principios fundamentales de confidencialidad, integridad, disponibilidad, continuidad del negocio y fortalecimiento de la cultura de seguridad. Sin embargo, se observa la necesidad de revisar dichos objetivos para alinearlos con el enfoque de resultados, medición del desempeño y gestión de riesgos promovido por la ISO/IEC 27001:2022 y por la Resolución 2277 de 2025, garantizando que sean medibles, verificables y consistentes con el contexto actual de amenazas y riesgos de la Entidad.
5. Manual del SGSI – Cumple	Las evidencias demuestran que la documentación del Sistema de Gestión de Seguridad de la Información hace parte del Sistema Integrado de Gestión y contempla los principales documentos que soportan la operación del SGSI. No obstante, considerando la expedición de la Resolución 2277 de 2025 y la transición hacia la **ISO/IEC 27001:2022**, resulta recomendable revisar y actualizar el manual para asegurar que la estructura documental incorpore los nuevos controles, conceptos y lineamientos establecidos en el Modelo de Seguridad y Privacidad de la Información.

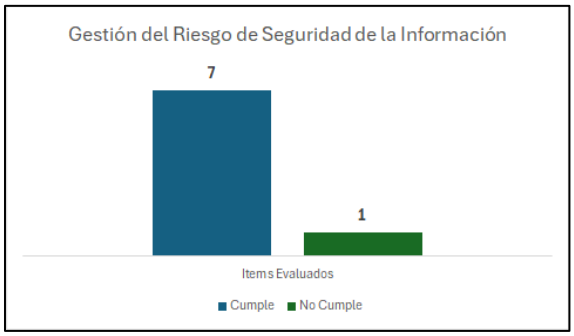
Requerimiento	Observación OCI
6. Roles y responsabilidades – Cumple Parcialmente	La Entidad ha definido responsabilidades para la Alta Dirección, la Oficina de Tecnologías de la Información, el Comité Institucional de Gestión y Desempeño, funcionarios y contratistas, evidenciando una distribución general de funciones dentro del SGSI. Sin embargo, se identificó la necesidad de fortalecer la asignación de responsabilidades conforme a los nuevos roles definidos por la Resolución 2277 de 2025, especialmente en aspectos relacionados con gobierno de la seguridad, gestión de riesgos, ciberseguridad y supervisión de controles.
7. Organigrama funcional – Cumple	Se verificó que la Entidad dispone de una estructura organizacional definida mediante el Decreto 4802 de 2011 y que la Oficina de Tecnologías de la Información cuenta con una organización funcional que incorpora el dominio de Seguridad de la Información. La evidencia presentada demuestra una adecuada identificación de las áreas responsables de la gestión del SGSI.
8. Designación del Oficial de Seguridad de la Información – No cumple	Aunque la Entidad manifiesta que el liderazgo técnico del SGSI es ejercido por un Profesional Especializado, no se evidenció un acto administrativo, resolución, memorando o documento formal que designe expresamente al Oficial de Seguridad de la Información, ni que establezca sus funciones, responsabilidades y autoridad dentro del sistema. La designación formal de este rol constituye una buena práctica de gobierno y fortalece la independencia, trazabilidad y responsabilidad en la administración del SGSI.
9. Comité de Seguridad de la Información – Cumple	Se verificó la existencia de actas del Comité Institucional de Gestión y Desempeño donde se abordaron asuntos relacionados con el SGSI, incluyendo la aprobación del PESI y del Plan de Tratamiento de Riesgos. La evidencia demuestra que existe un mecanismo institucional para la toma de decisiones estratégicas en materia de seguridad de la información.
10. Indicadores del SGSI – Cumple	La Entidad dispone de indicadores asociados al desempeño del SGSI, orientados a medir aspectos como la efectividad de controles, gestión de vulnerabilidades, cultura de seguridad, continuidad del servicio y nivel de implementación del MSPI. Asimismo, se evidenciaron resultados de medición que permiten realizar seguimiento al desempeño del sistema y apoyar la toma de decisiones.

Requerimiento	Observación OCI
11. Revisión por la Dirección – No cumple	La evidencia presentada corresponde a una revisión efectuada durante la vigencia 2023, sin demostrarse la realización de revisiones periódicas posteriores conforme al ciclo de mejora continua del SGSI. De acuerdo con la ISO/IEC 27001:2022, la Alta Dirección debe revisar el desempeño del sistema de forma planificada y periódica para evaluar su eficacia, el estado de las acciones de mejora, los cambios en el contexto organizacional, los riesgos emergentes, el cumplimiento de objetivos y las necesidades de recursos. La ausencia de estas revisiones limita la capacidad de la Dirección para ejercer un gobierno efectivo sobre el SGSI y adoptar decisiones oportunas frente a cambios regulatorios, tecnológicos o de riesgo.

Gestión del Riesgo de Seguridad de la Información

En la revisión efectuada se evidencia que la entidad cuenta con una metodología para la gestión de riesgos de seguridad de la información, inventario de riesgos, controles definidos y planes de tratamiento, lo que demuestra una implementación alineada con los requisitos de la ISO/IEC 27001:2022.

No obstante, el análisis permite identificar dos aspectos por fortalecer. El primero corresponde a la gestión de riesgos asociados a servicios en la nube, ya que no se evidencian riesgos específicos relacionados con configuraciones inseguras, dependencia del proveedor, modelo de responsabilidad compartida o protección de la información en estos entornos. El segundo, y de mayor relevancia, es la gestión de riesgos asociados a terceros, debido a que la matriz no demuestra una identificación y tratamiento específico de los riesgos de seguridad derivados de proveedores, servicios tecnológicos o de la cadena de suministro, conforme a los controles A.5.19, A.5.20 y A.5.21 de la ISO/IEC 27001:2022.



Fuente OTI – Análisis OCI

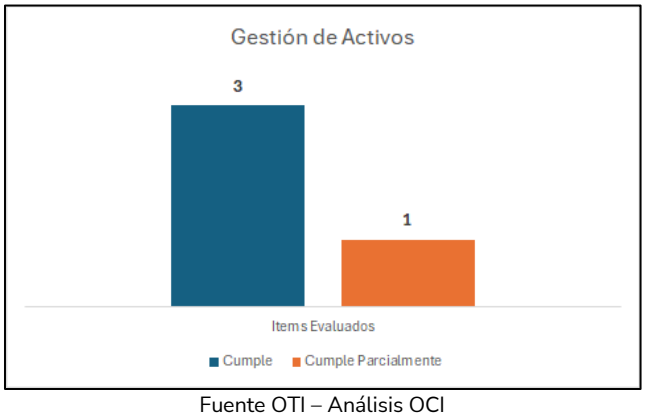
Requerimiento	Observación OCI
1. Metodología de Gestión del Riesgo - Cumple	Teniendo en cuenta los soportes aportados por el proceso, se verificó que la entidad aplica una metodología formal para la gestión de riesgos basada en buenas prácticas y es utilizada como marco de referencia para la identificación, análisis, evaluación y tratamiento de los riesgos de seguridad de la información. En consecuencia, se considera que el requisito evaluado se cumple. No obstante, se identifica como oportunidad de mejora la planificación de la transición hacia la versión más reciente de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas emitida por el Departamento Administrativo de la Función Pública, con el propósito de mantener la metodología institucional actualizada y alineada con los lineamientos vigentes.
2. Inventario de riesgos de Seguridad de la Información - Cumple	La evidencia aportada permite establecer que la entidad dispone de un inventario de riesgos de seguridad de la información para la vigencia 2026, en el que se encuentran identificados los riesgos, los controles implementados y los planes de acción definidos para su tratamiento. Asimismo, se evidenció la incorporación de riesgos estandarizados para las Direcciones Territoriales y su integración con el mapa de riesgos institucional. Con base en lo anterior, se concluye que el requisito evaluado se cumple, al existir un proceso formal para la identificación y gestión de los riesgos de seguridad de la información. Como oportunidad de mejora, se recomienda considerar la actualización de la metodología Institucional conforme a la versión vigente de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas emitida por el Departamento Administrativo de la Función Pública.
3. Matriz de riesgos de Seguridad de la Información - Cumple	El análisis de la información suministrada permite evidenciar que la entidad dispone de matrices de riesgos de seguridad de la información por proceso, debidamente actualizadas para la vigencia 2026 y estructuradas bajo criterios que contemplan la identificación del riesgo, su valoración, los controles implementados y la referencia a los controles aplicables del Anexo A de la ISO/IEC 27001:2022. De igual forma, se verificó su validación por parte de los responsables de los procesos, lo que proporciona evidencia suficiente para concluir que el requisito evaluado cumple. Como aspecto de mejora, se recomienda considerar la actualización de la metodología Institucional conforme a la versión vigente de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas emitida por el Departamento Administrativo de la Función Pública.
4. Planes de tratamiento - Cumple	La evaluación determinó que la entidad cuenta con planes de tratamiento formalmente definidos para los riesgos de seguridad de la información

Requerimiento	Observación OCI
	identificados, los cuales establecen actividades, responsables, fechas de ejecución y evidencias esperadas, permitiendo realizar el seguimiento a su implementación. Adicionalmente, se constató que estos planes fueron aprobados por el Comité Institucional de Gestión y Desempeño, lo que respalda su adopción dentro del SGSI. En consecuencia, se considera que el requisito evaluado se cumple
5. Evidencia del seguimiento efectuado - Cumple	Las evidencias demuestran que la entidad realiza el seguimiento a los riesgos de seguridad de la información mediante un mecanismo definido que permite verificar periódicamente la ejecución de los controles y el avance de los planes de tratamiento. Los reportes presentados evidencian la participación de los Enlaces SIG y el monitoreo de los riesgos en los procesos y Direcciones Territoriales. En consecuencia, se concluye que el requisito evaluado cumple
6. Riesgos aceptados por la Alta Dirección - Cumple	Las evidencias demuestran que la entidad cuenta con un proceso formal para la aceptación de los riesgos residuales, el cual se materializa mediante la aprobación del Plan de Tratamiento de Riesgos por parte del Comité Institucional de Gestión y Desempeño y la validación de las matrices por los líderes de proceso. Asimismo, se constató que los riesgos aceptados corresponden a niveles de severidad residual baja, de acuerdo con los criterios definidos en la metodología institucional. En consecuencia, se considera que el requisito evaluado se cumple, al evidenciarse la aceptación de los riesgos residuales por la instancia de gobierno competente.
7. Riesgos asociados a servicios en la nube - Cumple	La evidencia revisada permite establecer que la entidad ha incorporado riesgos relacionados con los servicios en la nube dentro de su matriz de riesgos de seguridad de la información, particularmente en aspectos asociados con la disponibilidad de la información, la gestión de identidades, el control de accesos y el uso de SharePoint y OneDrive como repositorios institucionales. En consecuencia, se considera que el requisito evaluado cumple. No obstante, como oportunidad de mejora, se recomienda ampliar el análisis de riesgos para incluir escenarios específicos de los servicios en la nube, tales como configuraciones inseguras, exposición de información, dependencia del proveedor, indisponibilidad del servicio, gestión de identidades, monitoreo de eventos y estrategias de salida (*exit strategy*), de conformidad con las buenas prácticas establecidas en la ISO/IEC 27001:2022, especialmente en el control A.5.23 – Seguridad de la información para el uso de servicios en la nube.
8. Riesgos asociados a terceros – No Cumple	Del análisis de la evidencia suministrada se concluye que el requisito no cumple. Si bien la entidad contempla la gestión de riesgos asociados a terceros desde la perspectiva del proceso contractual, no se evidenció una identificación, evaluación

Requerimiento	Observación OCI
	y tratamiento específico de los riesgos de seguridad de la información derivados de las relaciones con proveedores, operadores o terceros que acceden, procesan, almacenan o administran información institucional. Tampoco se aportó evidencia de la definición de requisitos de seguridad en los acuerdos con proveedores, evaluaciones periódicas de seguridad, mecanismos de seguimiento a su cumplimiento o controles asociados a la cadena de suministro de tecnologías de la información. Esta situación evidencia un cumplimiento parcial de los controles A.5.19, A.5.20 y A.5.21 del Anexo A de la ISO/IEC 27001:2022, los cuales requieren gestionar los riesgos de seguridad de la información durante todo el ciclo de relación con terceros.

Gestión de Activos

Conforme a la revisión efectuada se concluye que la entidad cuenta con mecanismos documentados para la identificación, clasificación y administración de los activos de información, así como también inventarios de infraestructura tecnológica y un catálogo de servicios que soportan la operación institucional. Estos elementos evidencian la implementación de controles orientados a la gestión de los activos de información, en concordancia con los requisitos establecidos en la ISO/IEC 27001:2022, particularmente en los controles A.5.9, A.5.12 y A.5.13 del Anexo A. En consecuencia, se considera que el requisito evaluado se cumple. No obstante, se identifican oportunidades de mejora relacionadas con la actualización permanente del catálogo de servicios tecnológicos y el fortalecimiento del inventario de activos mediante la incorporación de atributos como la criticidad, la identificación de activos administrados por terceros y su relación con los procesos de negocio, con el fin de incrementar la efectividad de la gestión de activos y del proceso de gestión de riesgos del SGSI.



Fuente OTI – Análisis OCI

Requerimiento	Observación OCI
1. **Inventario de activos de información - Cumple**	La evaluación determinó que la entidad mantiene un proceso formal para la administración y actualización del inventario de activos de información, articulado con los procesos institucionales y los Enlaces SIG. Asimismo, se verificó que los instrumentos de gestión de la información pública se encuentran aprobados por el Comité Institucional de Gestión y Desempeño y publicados conforme a los requisitos de la Ley 1712 de 2014. En consecuencia, se considera que el requisito evaluado cumple al demostrarse la existencia de mecanismos que permiten la identificación, actualización y administración de los activos de información, en concordancia con el control A.5.9 de la ISO/IEC 27001:2022.
2. Inventario de infraestructura tecnológica - Cumple	En la revisión efectuada se evidenció que la entidad mantiene un inventario de la infraestructura tecnológica integrado al inventario de activos de información, lo que permite identificar los componentes tecnológicos que soportan la operación institucional. En consecuencia, se considera que el requisito evaluado se cumple, al existir un mecanismo para la administración de estos activos en concordancia con el control A.5.9 de la ISO/IEC 27001:2022. No obstante, como oportunidad de mejora, se recomienda fortalecer el inventario mediante la clasificación de los activos según su modalidad de administración (propios, arrendados o administrados por terceros) e incorporar criterios de criticidad que faciliten la gestión del riesgo, la priorización de controles y la toma de decisiones sobre la infraestructura tecnológica.
3. Inventario de servicios tecnológicos - Cumple Parcialmente	Las evidencias demuestran que la entidad dispone de un catálogo de servicios tecnológicos administrado por la Mesa de Servicios de la Oficina de Tecnologías de la Información, el cual consolida los servicios prestados a los procesos y Direcciones Territoriales. No obstante, se evidenció que el documento aportado corresponde a la vigencia 2023, por lo que no refleja el estado actual de los servicios tecnológicos que soportan la operación institucional. En consecuencia, el requisito se considera parcialmente cumplido, dado que, si bien existe un instrumento para la gestión del catálogo de servicios, este requiere actualización para garantizar que la información sea vigente, confiable y útil para la administración de los servicios de TI y la gestión del SGSI.
4. Metodología de clasificación e identificación de activos.	Se evidencia que la entidad cuenta con una metodología formal para la identificación y clasificación de los activos de información, la cual define criterios de valoración basados en los principios de confidencialidad, integridad y disponibilidad, así como la identificación de activos críticos y la clasificación de la información de conformidad con la Ley 1712 de 2014. Adicionalmente, se verificó la existencia del procedimiento, el instructivo y los formatos que soportan su aplicación. En consecuencia, se considera que el requisito evaluado cumple con lo requerido al demostrarse que la entidad dispone de un marco metodológico

Requerimiento	Observación OCI
	documentado para la gestión y clasificación de los activos de información, en concordancia con los controles A.5.9 y A.5.12 de la ISO/IEC 27001:2022.

Gestión de Identidades y Accesos

Conforme a los soportes suministrados por el proceso se concluye que la entidad ha implementado controles para la gestión de identidades y accesos, incluyendo lineamientos de control de acceso, políticas de contraseñas, autenticación multifactor y mecanismos de administración de cuentas, lo que evidencia un avance en la adopción de los controles definidos en la ISO/IEC 27001:2022, especialmente los controles A.5.15 (Control de acceso), A.5.16 (Gestión de identidades), A.5.17 (Información de autenticación) y A.5.18 (Derechos de acceso).

Sin embargo, la evidencia revisada muestra oportunidades de mejora que limitan el cumplimiento integral de estos controles. En particular, no se evidenció una política de autenticación formalmente documentada e independiente, alineada con el Modelo de Seguridad y Privacidad de la Información; la documentación sobre la implementación de autenticación multifactor (MFA) no se demuestra su cobertura total en las plataformas institucionales; la relación de usuarios con privilegios no permite verificar claramente los roles, permisos y su justificación; y la revisión periódica de cuentas privilegiadas, cuentas genéricas y derechos de acceso no cuenta con evidencia suficiente que demuestre un proceso sistemático de validación y depuración.

En consecuencia, se concluye que la gestión de identidades presenta un nivel de implementación parcial, debido a que, aunque existen controles técnicos y administrativos en operación, la evidencia aportada no demuestra de forma integral su documentación, trazabilidad, revisión periódica y gobierno, aspectos necesarios para asegurar una administración eficaz de las identidades y accesos conforme a los requisitos de la ISO/IEC 27001:2022.

Requerimiento	Observación OCI
1. Política de autenticación - Cumple Parcialmente	Conforme al análisis efectuado se evidenció que la entidad dispone de lineamientos relacionados con el control de acceso y la autenticación, los cuales hacen parte de las Políticas Específicas de Seguridad de la Información y han sido fortalecidos mediante la implementación del proyecto de Gestión de Identidades. No obstante, el requisito se considera parcialmente cumplido, debido a que no se evidenció una política de autenticación formalmente documentada e independiente, que establezca de manera específica los lineamientos para la gestión de mecanismos de autenticación multifactor, credenciales, factores de autenticación y controles

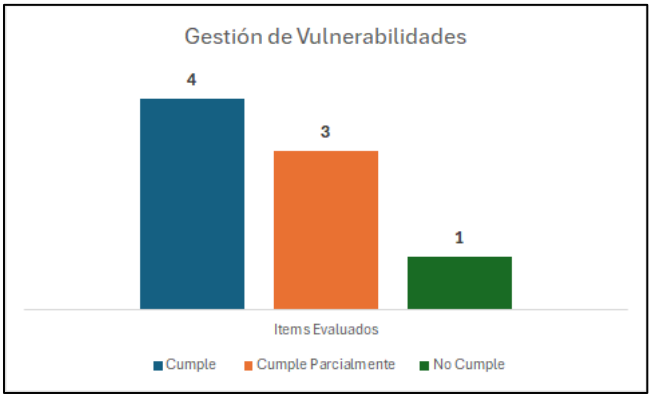
Requerimiento	Observación OCI
	asociados, conforme a lo previsto en el Modelo de Seguridad y Privacidad de la Información y al control A.5.17 – Información de autenticación de la ISO/IEC 27001:2022. En consecuencia, se recomienda formalizar este instrumento con el fin de fortalecer el marco de gobierno de la gestión de identidades y accesos.
2. Política de contraseñas - Cumple Parcialmente	La entidad cuenta con lineamientos para la gestión de contraseñas, los cuales se implementan mediante políticas de grupo (GPO) que establecen parámetros de complejidad, longitud mínima, vigencia, mantenimiento del historial y bloqueo por intentos fallidos. Sin embargo, el requisito se considera parcialmente cumplido, debido a que dichos lineamientos hacen parte de las Políticas Específicas de Seguridad de la Información y no se encuentran formalizados como una política específica de contraseñas, conforme a los lineamientos del Modelo de Seguridad y Privacidad de la Información adoptado mediante la Resolución 2277 de 2025. En consecuencia, se recomienda documentar y formalizar esta política, definiendo los criterios para la creación, uso, protección y administración de las credenciales de autenticación, en concordancia con el control A.5.17 – Información de autenticación de la ISO/IEC 27001:2022.
3. Política de autenticación multifactor - Cumple Parcialmente	Las evidencias demuestran que la entidad implementó la autenticación multifactor (MFA) para los servicios de Microsoft 365 y Azure, lo que evidencia la adopción de un mecanismo de autenticación robusta para proteger el acceso a los servicios institucionales. No obstante, el requisito se considera parcialmente cumplido, debido a que la evidencia suministrada se limita a demostrar la implementación técnica del control, sin aportar documentación que establezca su alcance, criterios de aplicación, excepciones, mecanismos de administración, monitoreo y revisión periódica. En consecuencia, se recomienda formalizar estos aspectos mediante procedimientos o lineamientos que soporten la gestión integral de la autenticación multifactor, en concordancia con los controles A.5.16 (Gestión de identidades) y A.5.17 (Información de autenticación) de la ISO/IEC 27001:2022.
4. Relación de usuarios con privilegios administrativos – No Cumple	El análisis permitió establecer que el requisito no se cumple. Si bien la entidad aportó la relación de usuarios con privilegios administrativos para Microsoft 365 y Azure, la información presentada no permite verificar el alcance de los privilegios asignados, los roles desempeñados, la justificación de los accesos, la aprobación de dichos permisos ni la existencia de revisiones periódicas sobre las cuentas privilegiadas. En consecuencia, la evidencia resulta insuficiente para demostrar una gestión adecuada de los accesos privilegiados, conforme a los controles A.5.15 (Control de acceso), A.5.16 (Gestión de identidades) y A.5.18 (Derechos de acceso) de la ISO/IEC 27001:2022, los cuales requieren que los privilegios sean autorizados, documentados, revisados y administrados durante todo su ciclo de vida.

Requerimiento	Observación OCI
5. Evidencia de revisión periódica de usuarios - Cumple Parcialmente	Se evidencia que la entidad realiza actividades de gestión sobre las cuentas de usuario, aportando la relación de usuarios creados durante la vigencia 2026 y una muestra de cuentas inactivadas en Microsoft 365. No obstante, el requisito se considera parcialmente cumplido, debido a que la evidencia no demuestra la existencia de un proceso formal y periódico de revisión de los derechos de acceso que permita validar la vigencia de las cuentas, la oportunidad en la desactivación de usuarios retirados y la pertinencia de los permisos asignados. Asimismo, se identificaron casos en los que la des habilitación de cuentas se realizó varios meses después del retiro del usuario y no se aportaron informes o registros que evidencien revisiones periódicas de los accesos. En consecuencia, se recomienda fortalecer el procedimiento de revisión de usuarios mediante controles periódicos y registros de seguimiento que permitan garantizar la gestión oportuna del ciclo de vida de las cuentas, en concordancia con los controles A.5.16 (Gestión de identidades) y A.5.18 (Derechos de acceso) de la ISO/IEC 27001:2022.
6. Relación de cuentas genéricas y su justificación- Cumple Parcialmente	Se concluye que el requisito se considera parcialmente cumplido. Si bien la entidad aportó la relación de cuentas genéricas de Microsoft 365 y evidenció la justificación para una de ellas, no se demostró que la totalidad de estas cuentas cuenten con una justificación documentada, una aprobación formal y una revisión periódica que valide la necesidad de mantenerlas activas. Asimismo, se identificaron cuentas institucionales que permanecen habilitadas sin que se aportara evidencia sobre su uso vigente o la justificación correspondiente. En consecuencia, se recomienda fortalecer el control de las cuentas genéricas mediante un proceso formal de autorización, revisión periódica y depuración, que garantice que su utilización responde a una necesidad operativa debidamente sustentada, en concordancia con los controles A.5.16 (Gestión de identidades), A.5.15 (Control de acceso) y A.5.18 (Derechos de acceso) de la ISO/IEC 27001:2022.
7. Evidencia de implementación de MFA en plataformas institucionales - Cumple Parcialmente	El requisito se considera parcialmente cumplido. Si bien la entidad aportó evidencias de la configuración e implementación de la autenticación multifactor (MFA) en Microsoft Entra ID y documentación sobre su despliegue en algunas plataformas institucionales, la información presentada no permite verificar que este mecanismo se encuentre implementado en la totalidad de los sistemas críticos ni demuestra la existencia de un proceso formal para su seguimiento, monitoreo y control. En consecuencia, se recomienda fortalecer la gestión del MFA mediante la definición de indicadores de cobertura, revisiones periódicas y registros que

Requerimiento	Observación OCI
	permitan verificar su aplicación y efectividad en todas las plataformas institucionales, en concordancia con los controles A.5.16 (Gestión de identidades), A.5.17 (Información de autenticación) y A.8.16 (Monitoreo de actividades) de la ISO/IEC 27001:2022.

Gestión de Vulnerabilidades

La evidencia revisada permite establecer que la entidad ejecuta actividades para la identificación y gestión de vulnerabilidades mediante herramientas de análisis, reportes técnicos y acciones de remediación, lo que demuestra la operación de controles orientados a reducir la exposición de la infraestructura tecnológica. Sin embargo, el análisis evidenció que el proceso aún presenta debilidades en su nivel de formalización, al no demostrar de manera consistente criterios documentados para la priorización de vulnerabilidades, tiempos de remediación según su criticidad, validación del cierre de los hallazgos y articulación con los procesos de gestión de cambios, incidentes y riesgos. En consecuencia, se concluye que la gestión de vulnerabilidades presenta un nivel de implementación parcial, debido a que, si bien existen actividades técnicas en ejecución, la evidencia no demuestra un proceso integral, medible y trazable que permita asegurar la gestión continua de las vulnerabilidades, conforme a los controles A.8.8 (Gestión de vulnerabilidades técnicas) y A.8.16 (Monitoreo de actividades) de la ISO/IEC 27001:2022.



Fuente OTI – Análisis OCI

Requerimiento	Observación OCI
1. Procedimiento de gestión de vulnerabilidades – No Cumple	De acuerdo con la verificación de las evidencias suministradas se concluye que el requisito no se cumple. Si bien la entidad realiza actividades para la identificación y análisis de vulnerabilidades mediante reportes de ColCERT y escaneos sobre la infraestructura tecnológica, la evidencia aportada no demuestra la existencia de un procedimiento formal de gestión de vulnerabilidades que establezca las actividades, responsabilidades, criterios de priorización, tiempos de remediación, validación del cierre de hallazgos y mecanismos de seguimiento. En consecuencia, las actividades ejecutadas corresponden a prácticas operativas, pero no evidencian un proceso documentado y estandarizado que garantice la gestión integral de las vulnerabilidades durante todo su ciclo de vida, conforme al control A.8.8 – Gestión de vulnerabilidades técnicas de la ISO/IEC 27001:2022.
2. Herramientas utilizadas – Cumple	La evidencia suministrada soporta que la entidad dispone de herramientas especializadas para la identificación y análisis de vulnerabilidades, entre ellas Microsoft Defender, Nessus, SecurityScorecard y Outpost24, complementadas con los reportes emitidos por ColCERT. Estas herramientas permiten fortalecer la detección de vulnerabilidades y el monitoreo de la postura de seguridad de la infraestructura tecnológica. En consecuencia, se considera que el requisito evaluado se cumple, al evidenciarse la implementación de herramientas técnicas que apoyan el proceso de gestión de vulnerabilidades, en concordancia con el control A.8.8 de la ISO/IEC 27001:2022.
3. Últimos informes de escaneo – Cumple Parcialmente	El análisis permitió establecer que el requisito se considera parcialmente cumplido. Si bien la entidad aportó informes de análisis de vulnerabilidades realizados sobre servidores, una muestra de estaciones de trabajo y ejercicios ejecutados por ColCERT, la evidencia no demuestra la aplicación de una metodología uniforme para la evaluación y priorización de los hallazgos en función de su criticidad. Asimismo, los informes revisados no evidencian de forma consistente los planes de remediación, los responsables, los tiempos de atención ni la validación del cierre de las vulnerabilidades identificadas. En consecuencia, se recomienda fortalecer la estructura y contenido de los informes de escaneo para asegurar la trazabilidad del ciclo de gestión de vulnerabilidades y facilitar la toma de decisiones basada en el nivel de riesgo, en concordancia con el control A.8.8 – Gestión de vulnerabilidades técnicas de la ISO/IEC 27001:2022.
4. Planes de remediación – Cumple	Con base a la evidencia suministrada se verificó que la entidad cuenta con una matriz para el seguimiento de las vulnerabilidades identificadas, la cual incorpora

Requerimiento	Observación OCI
	responsables, actividades de remediación, tiempos de implementación y seguimiento hasta el cierre de los hallazgos. Asimismo, se evidenció que este mecanismo permite priorizar las acciones de tratamiento de acuerdo con el impacto sobre la confidencialidad, integridad y disponibilidad de la información. En consecuencia, se considera que el requisito evaluado se cumple, al demostrarse la existencia de un mecanismo formal para la planificación, seguimiento y control de las acciones de remediación derivadas del proceso de gestión de vulnerabilidades, en concordancia con el control A.8.8 de la ISO/IEC 27001:2022.
5. Estado de vulnerabilidades críticas – Cumple Parcialmente	Conforme a los soportes aportados por el proceso responsable evidencia que el requisito se considera parcialmente cumplido. Si bien el informe emitido por ColCERT evidencia que no existen vulnerabilidades críticas abiertas en los sistemas de información y que las vulnerabilidades identificadas se encuentran en proceso de remediación, la información aportada no permite verificar de forma integral la trazabilidad de la gestión realizada sobre cada hallazgo, incluyendo su priorización, las acciones ejecutadas, la validación técnica del cierre y el seguimiento hasta su mitigación definitiva. En consecuencia, se recomienda fortalecer el registro y la trazabilidad del ciclo de vida de las vulnerabilidades, de manera que se pueda demostrar la efectividad de las acciones implementadas, en concordancia con el control A.8.8 – Gestión de vulnerabilidades técnicas de la ISO/IEC 27001:2022.
6. Evidencia del cierre de vulnerabilidades - Cumple	Se verificó que la entidad dispone de un mecanismo para registrar, gestionar y realizar seguimiento al cierre de las vulnerabilidades identificadas, soportado en una matriz de control y en los resultados de los análisis efectuados por ColCERT. Asimismo, la evidencia presentada demuestra que los hallazgos son incorporados al proceso de remediación y que, para el periodo evaluado, no se registraron vulnerabilidades críticas pendientes en los sistemas de información. En consecuencia, se considera que el requisito evaluado se cumple, al evidenciarse un proceso de seguimiento que permite verificar el tratamiento y cierre de las vulnerabilidades identificadas, en concordancia con el control A.8.8 – Gestión de vulnerabilidades técnicas de la ISO/IEC 27001:2022.
7. Informes de pruebas de penetración internas y externas - Cumple Parcialmente	La evaluación de la evidencia aportada permitió establecer que el requisito se considera parcialmente cumplido. Si bien la entidad presentó informes de análisis de vulnerabilidades internas y externas realizados sobre servidores, estaciones de trabajo y evaluaciones ejecutadas por ColCERT, la evidencia no demuestra que las pruebas de penetración y los análisis efectuados se desarrollen bajo una metodología estandarizada que permita valorar el nivel de exposición, priorizar los hallazgos según su criticidad y documentar de manera consistente las acciones de remediación. Asimismo, los informes revisados no evidencian de forma integral la trazabilidad entre los hallazgos identificados, las acciones correctivas

Requerimiento	Observación OCI
	implementadas y la validación de su cierre. En consecuencia, se recomienda fortalecer la documentación técnica y el contenido de los informes para asegurar una gestión integral de las vulnerabilidades, conforme al control A.8.8 – Gestión de vulnerabilidades técnicas de la ISO/IEC 27001:2022.
8. Seguimiento a hallazgos derivados de dichas pruebas – Cumple	La revisión de la evidencia aportada permitió verificar que la entidad documenta el seguimiento a los hallazgos identificados mediante una matriz de gestión de vulnerabilidades, la cual registra las acciones ejecutadas para su tratamiento y permite controlar el avance hasta su cierre. Este mecanismo proporciona trazabilidad sobre la gestión realizada y facilita el monitoreo de las actividades de remediación. En consecuencia, se considera que el requisito evaluado se cumple, al evidenciarse un proceso de seguimiento a los hallazgos derivados de los análisis de vulnerabilidades, en concordancia con el control A.8.8 – Gestión de vulnerabilidades técnicas de la ISO/IEC 27001:2022.

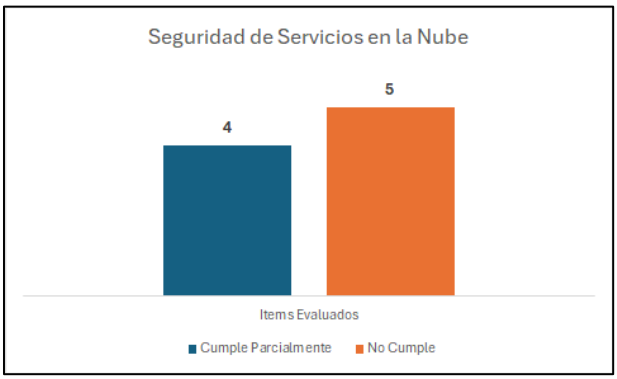
Seguridad de Servicios en la Nube

La revisión de la evidencia aportada permitió establecer que la entidad ha implementado controles de seguridad sobre su plataforma Microsoft Azure y Microsoft 365, incluyendo mecanismos de autenticación multifactor, políticas de acceso, configuraciones de respaldo, cifrado, registros de auditoría y monitoreo. No obstante, los soportes presentados corresponden principalmente a capturas de pantalla, reportes puntuales y documentos de trabajo, los cuales no permiten demostrar de manera integral el diseño, alcance, configuración y efectividad de los controles implementados.

Asimismo, no se evidenció un inventario técnico de los servicios en la nube, una arquitectura que permita identificar los componentes desplegados y sus relaciones, ni documentación que soporte la configuración de seguridad, los registros de auditoría, la gestión de logs, las políticas de respaldo y los mecanismos de cifrado implementados. Esta situación limita la trazabilidad de los controles y dificulta verificar su alineación con los riesgos asociados a los servicios en la nube.

En consecuencia, se concluye que la gestión de la seguridad de los servicios en la nube presenta un nivel de implementación parcial, debido a que, aunque existen controles técnicos en operación, la evidencia suministrada no demuestra de forma suficiente su documentación, administración y monitoreo conforme a los controles A.5.23 (Seguridad de la información para el uso de servicios en la nube), A.8.15 (Registro de eventos), A.8.16 (Monitoreo de actividades) y A.8.24 (Uso de la criptografía) de la ISO/IEC 27001:2022. Se recomienda fortalecer la

documentación técnica y la evidencia de los controles implementados para garantizar su trazabilidad, facilitar su evaluación y demostrar su efectividad dentro del SGSI.



Fuente OTI – Análisis OCI

Requerimiento	Observación OCI
1. Inventario de servicios Cloud utilizados – No Cumple	La información suministrada no proporciona evidencia suficiente para demostrar que la entidad dispone de un inventario de los servicios en la nube que permita su adecuada administración y control. Si bien se aportó un archivo como soporte del inventario, este no permite identificar ni caracterizar los servicios Cloud utilizados, su modelo de servicio (IaaS, PaaS o SaaS), el proveedor, los activos soportados, los responsables de su administración, la criticidad ni los controles de seguridad asociados. En consecuencia, el requisito no se cumple, debido a que la evidencia resulta insuficiente para gestionar de manera integral los servicios en la nube y los riesgos derivados de su utilización, conforme al control A.5.23 – Seguridad de la información para el uso de servicios en la nube de la ISO/IEC 27001:2022.
2. Arquitectura Cloud – Cumple Parcialmente	La evidencia presentada acredita la existencia de un documento relacionado con la arquitectura de los servicios en la nube; sin embargo, su contenido no permite identificar de manera clara la arquitectura tecnológica implementada por la entidad ni verificar aspectos como los servicios desplegados, su integración, los componentes que la conforman, los controles de seguridad aplicados y el modelo de responsabilidad compartida. En consecuencia, el requisito se considera parcialmente cumplido, toda vez que la información aportada no proporciona elementos suficientes para evaluar el diseño y la seguridad de la arquitectura de los servicios en la nube, conforme al control A.5.23 – Seguridad de la información para el uso de servicios en la nube de la ISO/IEC 27001:2022.

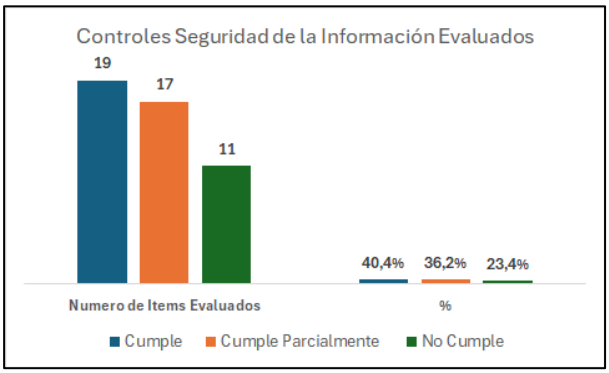
Requerimiento	Observación OCI
3. Configuración de seguridad – No Cumple	El soporte suministrado corresponde a un reporte de cobertura de aseguramiento en Microsoft Azure; sin embargo, su contenido no permite verificar la configuración de seguridad implementada sobre los servicios en la nube ni determinar el estado de los controles técnicos aplicados. Tampoco evidencia las configuraciones de línea base, las desviaciones identificadas, las acciones de remediación o el nivel de cumplimiento de las políticas de seguridad. En consecuencia, el requisito no se cumple, debido a que la información aportada resulta insuficiente para validar la configuración de seguridad de los servicios en la nube, conforme al control A.5.23 – Seguridad de la información para el uso de servicios en la nube de la ISO/IEC 27001:2022.
4. Evidencia de MFA – Cumple Parcialmente	La información suministrada evidencia que la entidad implementa autenticación multifactor (MFA) para el acceso a la plataforma Microsoft Azure, conforme a los lineamientos definidos para la gestión de identidades. No obstante, el requisito se considera parcialmente cumplido, debido a que la evidencia aportada no permite verificar de manera integral la configuración del control, su alcance sobre los servicios en la nube, las políticas de acceso condicional aplicadas, las excepciones definidas, ni los mecanismos de monitoreo y administración asociados. En consecuencia, se recomienda documentar y mantener actualizada la configuración técnica de las directivas de autenticación multifactor y su evidencia de operación, con el fin de demostrar la efectividad del control, en concordancia con los controles A.5.16 (Gestión de identidades), A.5.17 (Información de autenticación) y A.5.23 (Seguridad de la información para el uso de servicios en la nube) de la ISO/IEC 27001:2022.
5. Políticas de acceso – Cumple Parcialmente	La evidencia aportada demuestra que la entidad ha configurado directivas de acceso para Microsoft Azure y Microsoft 365, incorporando controles como la autenticación multifactor y restricciones de acceso basadas en la ubicación geográfica. No obstante, el requisito se considera parcialmente cumplido, debido a que las capturas de pantalla presentadas no permiten verificar de manera integral el alcance de las políticas implementadas, los usuarios o grupos a los que aplican, las condiciones de acceso definidas, las exclusiones autorizadas ni los mecanismos establecidos para su revisión y actualización. En consecuencia, se recomienda complementar la evidencia con la documentación técnica de las políticas de acceso y su administración, de manera que permita demostrar su diseño, implementación y efectividad, conforme a los controles A.5.15 (Control de acceso), A.5.16 (Gestión de identidades) y A.5.23 (Seguridad de la información para el uso de servicios en la nube) de la ISO/IEC 27001:2022.

Requerimiento	Observación OCI
6. Reportes de auditoría – No Cumple	Los soportes aportados permiten identificar que los servicios de auditoría de Microsoft Azure y Microsoft 365 se encuentran habilitados; sin embargo, el requisito no se cumple, debido a que la evidencia presentada no demuestra la operación efectiva. No se aportaron reportes de auditoría que permitan verificar la generación y conservación de registros, el monitoreo de eventos, el análisis de actividades relevantes ni el seguimiento a alertas de seguridad. En consecuencia, la información resulta insuficiente para demostrar que los registros de auditoría son utilizados como un mecanismo de detección, seguimiento y respuesta ante eventos de seguridad, conforme a los controles A.8.15 (Registro de eventos), A.8.16 (Monitoreo de actividades) y A.5.23 (Seguridad de la información para el uso de servicios en la nube) de la ISO/IEC 27001:2022.
7. Configuración de logs – Cumple Parcialmente	La documentación suministrada evidencia que la entidad ha configurado Log Analytics, Data Collection Rules y políticas de infraestructura para la recolección de registros en los servicios en la nube. No obstante, el requisito se considera parcialmente cumplido, debido a que la evidencia aportada no permite verificar el alcance de los registros generados, los eventos que son recopilados, los períodos de retención, los mecanismos de consulta y correlación, ni el uso de esta información para el monitoreo y la detección de eventos de seguridad. En consecuencia, se recomienda complementar la evidencia con documentación técnica y reportes que demuestren la operación y aprovechamiento de los registros generados, conforme a los controles A.8.15 (Registro de eventos), A.8.16 (Monitoreo de actividades) y A.5.23 (Seguridad de la información para el uso de servicios en la nube) de la ISO/IEC 27001:2022.
8. Configuración de respaldo – No Cumple	Las evidencias demuestran una política para la realización de copias de respaldo de servidores; sin embargo, el requisito no se cumple, debido a que la evidencia aportada no permite verificar la configuración de los respaldos sobre los servicios en la nube, su alcance, periodicidad, retención, cifrado, ubicación de almacenamiento, pruebas de restauración ni los mecanismos de monitoreo asociados. En consecuencia, la evidencia resulta insuficiente para demostrar que la estrategia de respaldo implementada protege la información alojada en la nube y garantiza su recuperación ante incidentes, conforme a los controles A.5.23 (Seguridad de la información para el uso de servicios en la nube), A.8.13 (Copias de respaldo) y A.5.30 (Preparación de las TIC para la continuidad del negocio) de la ISO/IEC 27001:2022.
9. Configuración de cifrado – No Cumple	La evidencia aportada se limita a una captura de pantalla de la configuración del cifrado de discos en Microsoft Azure; por lo tanto, el requisito no se cumple, esto debido a que esta información no permite verificar el alcance del cifrado implementado, los recursos protegidos, el mecanismo de administración de claves,

Requerimiento	Observación OCI
	las políticas aplicadas ni los procedimientos para su gestión y monitoreo. En consecuencia, la evidencia resulta insuficiente para demostrar que la entidad dispone de una estrategia documentada para la protección de la información mediante mecanismos criptográficos en los servicios en la nube, conforme a los controles A.8.24 (Uso de la criptografía) y A.5.23 (Seguridad de la información para el uso de servicios en la nube) de la ISO/IEC 27001:2022.

Resultados Evaluación Oficina de Control Interno

Dominio	Nivel
Gobierno SGSI	Parcial
Gestión Riesgos	Gestionado
Gestión Vulnerabilidades	Gestionado
Gestión Identidades	Gestionado
Cloud	Parcial
Mejora Continua	Parcial



Fuente OTI – Análisis OCI

La verificación realizada evidencia que la Entidad ha desarrollado un nivel importante de implementación de controles de seguridad de la información y dispone de elementos estructurales que soportan la operación del Sistema de Gestión de Seguridad de la Información (SGSI), tales como políticas institucionales, metodología de gestión de riesgos, inventarios de activos, mecanismos de autenticación, herramientas de monitoreo, procesos de remediación de vulnerabilidades y controles implementados sobre plataformas Microsoft 365 y Azure. Estas fortalezas demuestran un grado de madurez operacional que permite gestionar riesgos asociados a la seguridad de la información y mantener capacidades técnicas para la protección de los activos de información.

Sin embargo, el análisis también evidencia que el SGSI presenta brechas relevantes en su componente de gobierno, las cuales limitan la capacidad de la Alta Dirección para ejercer un liderazgo efectivo sobre la seguridad de la información. Las principales debilidades no se concentran en la inexistencia de controles técnicos, sino en la falta de actualización del marco

documental, la ausencia de formalización de roles críticos, la insuficiente evidencia de seguimiento estratégico y la limitada trazabilidad de la operación de varios controles. Esta situación genera una diferencia entre el nivel de implementación técnica y el nivel de madurez del sistema de gestión exigido por la ISO/IEC 27001:2022 y las regulaciones asociadas como las resoluciones 500 del 2021 y su actualización con la resolución 2277 del 2025.

Desde la perspectiva del Gobierno de Seguridad de la Información, se identifica que la organización continúa soportando parte de su estructura documental sobre lineamientos alineados con la ISO/IEC 27001:2013 y la Resolución 3157 de 2021, sin evidenciar una transición integral hacia los nuevos requisitos establecidos por la Resolución 2277 de 2025. Asimismo, persisten elementos esenciales sin formalizar, tales como el alcance del SGSI, la designación oficial del responsable de Seguridad de la Información y la revisión periódica por la Alta Dirección, aspectos que constituyen pilares del modelo de gobierno definido por la norma internacional. Estas situaciones limitan la capacidad institucional para demostrar liderazgo, asignación clara de responsabilidades y mejora continua del sistema.

En materia de gestión del riesgo, la Entidad evidencia una metodología consolidada y un proceso institucional para identificar, valorar y tratar riesgos de seguridad de la información; sin embargo, se observan oportunidades de fortalecimiento frente a riesgos emergentes asociados a servicios en la nube y, especialmente, a riesgos derivados de terceros y de la cadena de suministro. La ausencia de una evaluación específica sobre proveedores tecnológicos representa una exposición significativa, considerando la creciente dependencia de servicios externos y las obligaciones establecidas en los controles A.5.19, A.5.20 y A.5.21 de la ISO/IEC 27001:2022 y el Modelo de Seguridad y Privacidad de la Información.

Respecto a la gestión de identidades y accesos, se observa que existen controles tecnológicos implementados, incluyendo autenticación multifactor y administración de cuentas; sin embargo, la evidencia no demuestra un modelo integral de gobierno de identidades. Persisten debilidades relacionadas con la formalización de políticas específicas de autenticación, administración de privilegios, revisión periódica de derechos de acceso, justificación de cuentas genéricas y demostración de cobertura integral del MFA sobre los sistemas críticos. Estas condiciones incrementan el riesgo de accesos indebidos y reducen la capacidad institucional para demostrar el adecuado control del ciclo de vida de las identidades digitales.

La evaluación de los servicios en la nube constituye el componente con mayor nivel de oportunidad de mejora. Aunque se evidencian controles técnicos implementados en Microsoft Azure y Microsoft 365, la documentación suministrada no permite demostrar de manera

suficiente el diseño, alcance, configuración y monitoreo de dichos controles. La ausencia de inventarios técnicos, arquitecturas documentadas, configuraciones de seguridad, evidencias de auditoría, estrategias de respaldo y administración criptográfica limita la trazabilidad del entorno Cloud y dificulta verificar el cumplimiento integral del control A.5.23 de la ISO/IEC 27001:2022. En este componente predominan evidencias operativas basadas en capturas de pantalla y configuraciones puntuales, sin el soporte documental necesario para demostrar la gestión integral de la seguridad en servicios en la nube.

6. ANÁLISIS DEL COMPORTAMIENTO HISTORICO.

La presente evaluación constituye el primer ejercicio integral de seguimiento institucional realizado por la Oficina de Control Interno para verificar el nivel de implementación y madurez de los controles del Sistema de Gestión de Seguridad de la Información (SGSI), tomando como referencia los requisitos establecidos en la NTC ISO/IEC 27001:2022, el Modelo de Seguridad y Privacidad de la Información (MSPI) y los lineamientos definidos en la Resolución 2277 de 2025.

En este contexto, no es posible efectuar un análisis del comportamiento histórico ni establecer tendencias de evolución respecto al grado de implementación y efectividad de los controles evaluados, debido a que la Entidad no dispone de evaluaciones integrales anteriores bajo el marco de la ISO/IEC 27001:2022, ni de indicadores de línea base, mediciones de madurez, resultados comparativos o informes históricos que permitan determinar la evolución del Sistema de Gestión de Seguridad de la Información desde una perspectiva homogénea.

Esta situación obedece, principalmente, a la adopción de los nuevos lineamientos del Modelo de Seguridad y Privacidad de la Información establecidos mediante la Resolución 2277 de 2025 y a que la presente evaluación corresponde al primer ejercicio desarrollado por la Oficina de Control Interno con un enfoque integral sobre los componentes de gobierno, gestión del riesgo, gestión de activos, gestión de identidades y accesos, gestión de vulnerabilidades y seguridad de los servicios en la nube, conforme a los requisitos de la ISO/IEC 27001:2022.

En consecuencia, los resultados obtenidos constituyen la línea base institucional para futuras evaluaciones del Sistema de Gestión de Seguridad de la Información, permitiendo establecer, en ejercicios posteriores, análisis comparativos sobre el nivel de madurez, la eficacia de los controles implementados, el fortalecimiento del gobierno de la seguridad de la información y el avance en el cumplimiento de los requisitos normativos y de las mejores prácticas internacionales. No obstante, es importante precisar que los análisis, conclusiones y resultados contenidos en el presente informe corresponden a la evaluación de las evidencias objetivas suministradas por las

dependencias responsables durante el periodo auditado, por lo que reflejan el estado de implementación demostrado al momento de la auditoría.

7. ENFOQUE BASADO EN RIESGOS.

El enfoque de seguimiento aplicado permitió evaluar no solo la existencia de políticas, procedimientos, controles técnicos y administrativos asociados al Sistema de Gestión de Seguridad de la Información (SGSI), sino también determinar su nivel de implementación, formalización, trazabilidad y efectividad frente a los requisitos establecidos en la NTC ISO/IEC 27001:2022, el Modelo de Seguridad y Privacidad de la Información (MSPI) y la Resolución 2277 de 2025.

En consecuencia, con base en el estado actual evidenciado durante la auditoría, se identifican los siguientes riesgos potenciales a los cuales la Entidad podría encontrarse expuesta:

Tipo de Riesgo	Descripción	Posibles Consecuencias
Riesgo Estratégico	Posibilidad de que el Sistema de Gestión de Seguridad de la Información no alcance el nivel de madurez requerido, debido a debilidades en el gobierno del SGSI, ausencia de actualización del marco documental conforme a la ISO/IEC 27001:2022 y la Resolución 2277 de 2025, así como limitaciones en el direccionamiento estratégico y seguimiento por parte de la Alta Dirección.	Incumplimiento de requisitos normativos, debilidades en la toma de decisiones, disminución de la capacidad institucional para gestionar los riesgos de seguridad de la información.
Riesgo Tecnológico	Posibilidad de afectación de la infraestructura tecnológica y de los servicios institucionales por la inexistencia de procedimientos formalizados para la gestión de vulnerabilidades, insuficiente documentación técnica de los controles implementados y limitaciones en la gestión de la infraestructura tecnológica y los servicios en la nube.	Incremento de vulnerabilidades explotables, indisponibilidad de servicios, afectación de la continuidad operativa y aumento de la superficie de ataque.
Riesgo Asociado a Servicios en la Nube	Posibilidad de que los servicios Cloud utilizados por la Entidad no cuenten con una gestión integral de	Exposición de información institucional, pérdida de trazabilidad, indisponibilidad de

	seguridad, debido a la ausencia de inventarios técnicos, documentación de arquitectura, configuración de controles, administración de registros, respaldos, cifrado y monitoreo de los servicios en la nube.	servicios, incumplimiento de controles establecidos en la ISO/IEC 27001:2022.
Riesgo Asociado a Terceros y Cadena de Suministro	Posibilidad de materialización de incidentes de seguridad derivados de proveedores, operadores tecnológicos o terceros que administran, procesan o acceden a información institucional, debido a la inexistencia de una gestión específica de riesgos, controles de seguridad y mecanismos de seguimiento durante la relación contractual.	Incidentes originados en terceros, fuga de información, incumplimientos contractuales, afectación de la continuidad del servicio y aumento del riesgo de ciberataques.
Riesgo de Cumplimiento	Posibilidad de incumplir los requisitos establecidos en la NTC ISO/IEC 27001:2022, el Modelo de Seguridad y Privacidad de la Información, la Resolución 2277 de 2025 y demás disposiciones aplicables en materia de seguridad digital y protección de la información, debido a deficiencias en la actualización documental y en la evidencia de implementación de los controles.	Observaciones de organismos de control, incumplimiento normativo, hallazgos de auditoría y posibles responsabilidades administrativas.

8. CONCLUSIONES DEL ANÁLISIS Y VALIDACIÓN DE EVIDENCIAS

Con fundamento en las evidencias suministradas por la dependencia responsable, las pruebas de revisión ejecutadas y los criterios establecidos en la NTC ISO/IEC 27001:2022, el Modelo de Seguridad y Privacidad de la Información (MSPI) y la Resolución 2277 de 2025, la Oficina de Control Interno concluye que la Entidad ha desarrollado avances importantes en la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), evidenciando la existencia de políticas, metodologías, procedimientos, controles técnicos y mecanismos de gestión orientados a proteger la confidencialidad, integridad y disponibilidad de la información institucional.

La evaluación permitió identificar que las principales brechas no están asociadas a la inexistencia de controles técnicos, sino a debilidades en el gobierno del SGSI, la actualización del marco documental, la formalización de procesos, la gestión de riesgos emergentes y la evidencia que demuestra la eficacia de los controles implementados, aspectos que limitan el nivel de madurez del sistema y su alineación con los requisitos de la ISO/IEC 27001:2022.

Entre los aspectos más relevantes identificados se encuentran la necesidad de actualizar las políticas y demás documentos del SGSI conforme a la Resolución 2277 de 2025, formalizar el alcance del sistema, fortalecer el liderazgo y las responsabilidades de gobierno, realizar revisiones periódicas por la Alta Dirección, robustecer la gestión de riesgos asociados a terceros y servicios en la nube, consolidar el gobierno de identidades y accesos, formalizar el procedimiento de gestión de vulnerabilidades y mejorar la documentación y trazabilidad de los controles implementados.

9. CONCEPTO DE CONTROL INTERNO.

Como resultado de la evaluación independiente realizada, la Oficina de Control Interno concluye que el Sistema de Gestión de Seguridad de la Información (SGSI) en lo relacionado con la gestión de los controles presenta un nivel de implementación funcional con un grado de madurez parcial, evidenciando la existencia de controles administrativos y técnicos que soportan la gestión de la seguridad de la información; sin embargo, persisten brechas estructurales que limitan la eficacia del sistema para garantizar el cumplimiento integral de los requisitos establecidos en la NTC ISO/IEC 27001:2022, el Modelo de Seguridad y Privacidad de la Información (MSPI) y la Resolución 2277 de 2025.

La evaluación permitió establecer que la Entidad dispone de mecanismos para la gestión de riesgos, administración de activos, control de identidades, gestión de vulnerabilidades y protección de los servicios tecnológicos; no obstante, las evidencias analizadas demuestran oportunidades de mejora en los componentes de gobierno, direccionamiento estratégico, formalización documental, gestión de riesgos emergentes, monitoreo y demostración de la efectividad de los controles, aspectos esenciales para asegurar la operación y mejora continua del SGSI.

Desde la perspectiva del Sistema de Control Interno, el principal nivel de exposición no se origina por la ausencia de controles tecnológicos, sino por las debilidades identificadas en su institucionalización, integración con el modelo de gobierno, trazabilidad, seguimiento y evaluación de desempeño, lo que reduce la capacidad de la Alta Dirección para ejercer un

gobierno efectivo sobre la seguridad de la información y limita la generación de evidencia objetiva que demuestre la eficacia de los controles implementados.

En consecuencia, la Oficina de Control Interno considera que el SGSI requiere fortalecer prioritariamente su modelo de gobierno, la actualización del marco normativo y documental, la gestión integral de riesgos asociados a terceros y servicios en la nube, el gobierno de identidades y accesos, la formalización de la gestión de vulnerabilidades y los mecanismos de monitoreo y revisión por la Alta Dirección, con el propósito de incrementar el nivel de madurez institucional, asegurar la sostenibilidad de los controles implementados y consolidar un sistema alineado con el enfoque de gestión basada en riesgos y mejora continua previsto en la ISO/IEC 27001:2022.

APROBÓ _____

JEFE OFICINA DE CONTROL INTERNO

Elaborado: Basco Ricaurte Guerra
Contratista Oficina de Control Interno

Anexo 1 Control de cambios

Versión	Fecha de Cambio	Descripción de la modificación
1	04/08/2014	Creación del formato.
2	09/03/2015	Al revisar el formato se evidencia que la casilla fecha de informe está repetida.
3	02/08/2017	Se modifica formato y se adiciona firma aprobación del jefe Oficina de Control Interno.
4	30/04/2020	Se actualiza formato, se ajusta la distribución del texto en filas y columnas, las fuentes y fecha de la tabla control de cambios.
5	28/10/2022	Se actualiza el formato en pie de página con los logos de certificación asociados al sistema de gestión de calidad ISO 9001:2015,

		ambiental ISO 14001:2015, seguridad y salud en el trabajo ISO 45001:2018 seguridad de la información ISO 27001:2013.
6	19/07/2024	Se actualiza el formato es su estructura de contenido, de acuerdo con los requerimientos de la Oficina de Control Interno.