| Fecha de Emisión del Informe | Día | 27 | Mes | 04 | Año | 2026 |
|---|---|---|---|---|---|---|

| | |
|---|---|
| **Número de Informe:** | 1/1 |
| **Nombre:** | Informe de Seguimiento a la disponibilidad, confiabilidad, integridad y seguridad de la información requerida para la prestación del servicio. |
| **Objetivo:** | Realizar el seguimiento y la evaluación del avance en la implementación del Sistema de Gestión de Seguridad de la Información, teniendo en cuenta los principios de disponibilidad, confiabilidad e integridad de la información. |
| **Alcance:** | Se inicia con la solicitud y recopilación de la información y concluye con el informe de evaluación al avance de la implementación del Sistema de Gestión de Seguridad de la Información SGSI en sus dimensiones de disponibilidad, confiabilidad e Integridad de la Información |
| **Periodicidad:** | El informe se debe realizar una (1) vez en el año, con corte a 31 de diciembre de la vigencia anterior. El actual informe corresponde con corte a diciembre 31 del 2025. |

## 1. MARCO JURÍDICO.

El marco normativo está relacionado con los requisitos usados como referencia al presente informe al seguimiento a los riesgos que están asociados a la seguridad de la información reservada y clasificada:

- **Ley 87 de 1993** "Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones"

- **Decreto 1499 de 2017** "Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015"

- **Guía para la Administración del Riesgo** y el diseño de controles en entidades públicas Versión 6

- **Resolución 0569 del 2017** "Por la cual se deroga la Resolución 0893 del 02 de septiembre de 2013 y se adopta el Sistema Integrado de Gestión de la Unidad para la Atención y Reparación Integral a las Victimas"

- **Decreto 1008 de 2018** "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078

de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"

- **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 y se dictan otras disposiciones".

- Manual Operativo del Componente de la Gestión de Seguridad de la Información (GSI) V10.

- Marco de Arquitectura Empresarial de TI – MinTic

**Marco normativo del modelo integrado de planeación y gestión - MIPG**

**1ª. Dimensión: Talento Humano**

**1.3 Política de Integridad**

la apropiación de los valores del servicio público.

fortalecer e integrar mecanismos, instrumentos administrativos y orientaciones que garanticen la idoneidad en la prestación del servicio

**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 GESTIÓN – MIPG.

Este informe de seguimiento presenta los avances a la implementación del Sistema de Gestión de Seguridad de la Información 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 presente informe de seguimiento tiene como objetivo presentar los resultados del análisis, evaluación y monitoreo del avance en la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), con corte al 31 de diciembre de 2025. El análisis se centra en los componentes clave del sistema: disponibilidad, confiabilidad e integridad de la información.

Se verifica el cumplimiento de las actividades planificadas, gestionadas y reportadas, conforme a los entregables establecidos en cada uno de los proyectos vinculados a la implementación del SGSI. La evaluación se realiza con base en la evidencia documentada, las metas definidas y los avances alcanzados en relación con los objetivos de seguridad de la información establecidos por la Entidad.

El informe está dirigido a la Dirección General y sus dependencias interesadas. Son también destinatarios los entes de control y a los ciudadanos en general que deseen hacer control social.

## 4. CONTEXTO DEL INFORME.

En el contexto de las Entidades Públicas, los sistemas de gestión adquieren una importancia estratégica, ya que permiten controlar, planificar, organizar y automatizar sus operaciones, garantizando así una mayor eficiencia y efectividad en la gestión institucional. Estos sistemas contribuyen significativamente a la mejora continua de los procesos, a la reducción de costos operativos, y al cumplimiento de los requisitos gubernamentales y legales. Además, proporcionan herramientas clave para facilitar la toma de decisiones informadas, fortaleciendo la transparencia, la rendición de cuentas y la optimización de los recursos públicos.

La Oficina de Control Interno en cumplimiento de sus funciones a determinado realizar una evaluación de los avances que se han gestionado a la implementación del Sistema de Gestión de Seguridad de la Información, teniendo en cuenta la responsabilidad de los procesos, determinando las principales brechas e impactos a los que puede estar expuesta la Entidad en cuanto a seguridad de la información.

## 5. RESULTADOS DEL ANÁLISIS Y VALIDACIÓN DE EVIDENCIAS.

La Oficina de Control Interno mediante correo electrónico del martes 10 de marzo se solicitó al líder de proceso de la *Oficina de Tecnologías de la Informacion* los avances en la implementación del Sistema de Gestión de Seguridad de la Información, las actividades ejecutadas en los diferentes proyectos asociados al SGSI, adicionalmente se envía una matriz en donde se solicita por parte de la OCI aspectos relacionados.

Al anterior requerimiento se recibió respuesta por parte de la Oficina de Tecnologías de la Información el miércoles 18 de marzo a las 14:17 en donde indica:

> *En atención a su solicitud, desde la Oficina de Tecnologías de la Información se remite la matriz diligenciada con la relación de enlaces habilitados para el acceso a las cuentas:*

*A continuación, enlaces compartidos:*

***PESI Operación***

*https://unidadvictimas.sharepoint.com/:f:/s/ISO270012013/IgC2tNuW6jmOToqZhXB_gNZvAWx7Wn5aaSXssocWg4GHSzM?e=EPe5Xh*

***PESI Proyectos:***

*Gestión de identidades (Ejecución):*

*https://unidadvictimas.sharepoint.com/:f:/s/GerenciadeProyectosOTI/IgD15qtkp09UR6-Rlty9KUhjAfOOZjCtgOdgit14Y7UY_V4?e=4hvW39*

*Datos Personales:*

*https://unidadvictimas.sharepoint.com/:f:/s/GerenciadeProyectosOTI/IgCRQf_EnBPrQLfRPV7RdEY2ATgCEugjtX_H056qLdcgM-U?e=nEniyu*

*Seguridad Perimetral y DLP:*

*https://unidadvictimas.sharepoint.com/:f:/s/GerenciadeProyectosOTI/IgBiW9vYORDbSLhROLiQ7SX0AazUqy4hCMN0OZ51frtWAq4?e=MjMMhF*

***Evidencias - Plan de Tratamiento de Riesgos:***

*Procesos:*

*https://unidadvictimas.sharepoint.com/:f:/s/ISO270012013/IgCMk44n4PvaRpo1YijDXP--ASXO109c84AGKJyMAsjSM64?e=BTMjly*

*Direcciones Territoriales:*

*https://unidadvictimas.sharepoint.com/:f:/s/ISO270012013/IgANfDKo-cE5RLEZKYxx47uYAacxZPOrfUIgF7EhesG1n_k?e=EPGa8y*

***Seguimiento PESI:***

*https://unidadvictimas.sharepoint.com/:f:/s/ISO270012013/IgAQgGJ_PCTvRLijEe9U6VKHAfTK9XF3lUuxLNfeMbqt1Ek?e=B0PxAP*

*En este sentido, indico que el Ingeniero Joaquín Rojas Palomino atenderá las inquietudes que puedan surgir en el proceso de revisión de la información.*

Adicionalmente, la Oficina de Control Interno solicito la aclaración y complementación de la información entregada bajo correo electrónico de fecha 06 de abril a las 9:57 a.m., de la cual se recibió respuesta por el enlace asignado por el líder del proceso el día 08 de abril a las 17:09 p.m.

**5.1 Análisis de la Informacion Oficina de Control Interno**

A la fecha de corte del seguimiento se presenta por parte de los responsables de los procesos los avances que se han realizado en los diferentes proyectos que están asociados a la implementación del Sistema de Gestión de Seguridad de la Información y que se ejecutaron en el marco del Plan Estratégico de Seguridad de la Información – PESI de la vigencia 2025 relacionados de manera directa y transversal con los principios de seguridad de la información sobre disponibilidad, confiabilidad e Integridad de la Información.

A continuación, se relacionan las acciones o proyectos ejecutados en la vigencia 2025 en donde estos son clasificados teniendo en cuenta los principios de seguridad de la información y se emiten las respectivas observaciones a la revisión de los soportes aportados por el proceso de la siguiente manera:

| No. | Principios SGSI | Política Asociada | Numeral Política - Resolución 3157 de 2021 | Acción o Proyecto Ejecutado | Objetivo | Fecha de Inicio | Fecha de Terminación | % de avance | Estado | Observaciones OCI |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Confidencialidad/Integridad / Disponibilidad | Resolución 3157 de 2021 Artículo 2 - Política General del Sistema de Gestión de Seguridad de la Información | Transversal | PESI Operación: Realizar la actualización (en caso de ser necesario) y socialización de políticas, procedimientos y/o protocolos de seguridad de la información (CID) | Objetivo Resolución 3157 de 2021: A. Proteger la información y sistemas de información, según estándares que salvaguarden la confidencialidad, integridad y disponibilidad, de los activos de la Entidad.<br><br>Objetivo específico: Gestionar la actualización de la documentación del SGSI, según lo establecido en el MSPI del MinTIC y lo contemplado en la actualización del PESI aprobado por el Comité Institucional de Gestión y Desempeño | 1/02/2025 | 31/10/2025 | 100% | Cerrado | Se evidencia que se llevaron a cabo las acciones planteadas para la actualización de la documentación correspondiente. No obstante, se recomienda implementar instrumentos de seguimiento y control que permitan garantizar la trazabilidad de las gestiones y acciones realizadas durante cada vigencia.<br><br>Adicionalmente, se sugiere la creación de un repositorio único que permita clasificar y organizar la información de acuerdo con las etapas o fases definidas, tales como: revisión y actualización, aprobación, envío a OAP, correcciones y versiones finales. |

| No. | Principios SGSI | Política Asociada | Numeral Política - Resolución 3157 de 2021 | Acción o Proyecto Ejecutado | Objetivo | Fecha de Inicio | Fecha de Terminación | % de avance | Estado | Observaciones OCI |
|---|---|---|---|---|---|---|---|---|---|---|
| 2 | Confidencialidad/Integridad / Disponibilidad | Resolución 3157 de 2021 Artículo 2 - Política General del Sistema de Gestión de Seguridad de la Información | Artículo 2. Política General del Sistema de Gestión de Seguridad de la Información | Gestionar la implementación de políticas y controles de seguridad de la información aplicables a los procesos y Direcciones Territoriales (CID) | Objetivo Resolución 3157 de 2021: 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 de la Entidad.<br><br>Objetivo específico: Gestionar la implementación progresiva de políticas y controles de seguridad en la Entidad | 1/02/2025 | 30/11/2025 | 100% | Cerrado | Si bien se evidencian las actividades realizadas en la gestión de seguridad de la información, estas corresponden en su mayoría a la atención de incidencias y a la actualización de parámetros previamente establecidos en los diferentes instrumentos y herramientas, en el marco de la operación de seguridad.<br><br>No obstante, se recomienda que, para la implementación de políticas y controles, se realice previamente un análisis de las principales brechas existentes. Con base en este diagnóstico, se sugiere definir un roadmap que permita orientar el fortalecimiento y el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI). |
| 3 | Confidencialidad/Integridad / Disponibilidad | Resolución 3157 de 2021 Artículo 2 - Política General del Sistema de Gestión de Seguridad de la Información | Artículo 11. Política de seguridad de las operaciones.<br><br>Numeral 10.<br><br>Artículo 15. Política de gestión de incidentes de seguridad de la información. | Realizar la atención y seguimiento a los eventos e incidentes de seguridad de la información (CID) | Objetivo Resolución 3157 de 2021: C. Realizar seguimiento a los eventos e incidentes de seguridad para obtener lecciones aprendidas y mejorar periódicamente el sistema de gestión de Seguridad de la Información. | 1/01/2025 | 31/12/2025 | 100% | Cerrado | Se evidencia que la gestión de eventos e incidentes de seguridad de la información se limita a la atención y resolución de los casos reportados. Sin embargo, no se identifican actividades orientadas al análisis posterior de dichos eventos, tales como la generación de lecciones aprendidas, identificación de causas raíz o la definición de acciones de mejora.<br><br>En consecuencia, no se está dando cumplimiento al lineamiento establecido, ya que no se realiza un seguimiento integral que permita retroalimentar y fortalecer de manera periódica el Sistema de Gestión de Seguridad de la Información (SGSI). Se recomienda implementar mecanismos formales de análisis y evaluación de incidentes que contribuyan al mejoramiento continuo del sistema, se recomienda la implementación de informes de gestión de esta actividad donde se incluyan los parámetros de medición y análisis respectivos. |

| No. | Principios SGSI | Política Asociada | Numeral Política - Resolución 3157 de 2021 | Acción o Proyecto Ejecutado | Objetivo | Fecha de Inicio | Fecha de Terminación | % de avance | Estado | Observaciones OCI |
|---|---|---|---|---|---|---|---|---|---|---|
| 4 | Integridad / Disponibilidad | Resolución 3157 de 2021 Artículo 2 - Política General del Sistema de Gestión de Seguridad de la Información | Artículo 16. Política de gestión de la continuidad de negocio. | Gestionar la ejecución de pruebas de Continuidad de la Operación Tecnológica (ID) | Objetivo Resolución 3157 de 2021: E. Incrementar la disponibilidad de servicios de TI y de operación, a través del plan de continuidad de negocio | 1/02/2025 | 30/11/2025 | 100% | Cerrado | La información corresponde a las acciones planeadas, se recomienda para próximos informes ajustar la forma en donde se incluya un índice de tablas y de imágenes, adicionalmente verificar que las imágenes estén legibles. |
| 5 | Confidencialidad | Resolución 3157 de 2021 Artículo 2 - Política General del Sistema de Gestión de Seguridad de la Información | Artículo 7. Política de gestión de activos. | Actualizar inventario de activos de información y gestionar la publicación de los instrumentos de gestión de información en página Web Institucional © | Objetivo Resolución 3157 de 2021: A. Proteger la información y sistemas de información, según estándares que salvaguarden la confidencialidad, integridad y disponibilidad, de los activos de la Entidad.<br><br>Objetivo específico: Gestionar la actualización del inventario de activos de información según el procedimiento establecido | 1/03/2025 | 31/10/2025 | 100% | Cerrado | Sin Observaciones |
| 6 | Confidencialidad/Integridad / Disponibilidad | Resolución 3157 de 2021 Artículo 2 - Política General del Sistema de Gestión de Seguridad de la Información | Artículo 4. Política de organización interna<br><br>(Transversal En su gestión se abordan controles y planes de tratamiento) | Identificar, valorar y evaluar los Riesgos de Seguridad de la información y definir el correspondiente plan de tratamiento y realizar seguimiento con respecto a las evidencias de controles, riesgos y planes de tratamiento al riesgo (Ejecución del plan de tratamiento de Riesgos) (CID) | Objetivo Resolución 3157 de 2021: 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 de la Entidad. | 1/05/2025 | 30/11/2025 | 100% | Cerrado | Se debe actualizar la información que hace falta de los procesos que gestionaron una nueva versión de los riesgos de seguridad de la información, o reportar los que no realizaron el ejercicio |
| 7 | Confidencialidad/Integridad / Disponibilidad | Resolución 3157 de 2021 Artículo 2 - Política General del Sistema de Gestión de Seguridad de la Información | Artículo 2. Política General del Sistema de Gestión de Seguridad de la Información<br><br>(Transversal En su gestión se abordan la totalidad de controles) | Realizar diagnóstico técnico de implementación de controles de seguridad aplicables al Proceso, de acuerdo con la Declaración de aplicabilidad (SOA) (CID) | Objetivo Resolución 3157 de 2021: 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 de la Entidad. | 1/03/2025 | 30/09/2025 | 100% | Cerrado | Sin Observaciones |

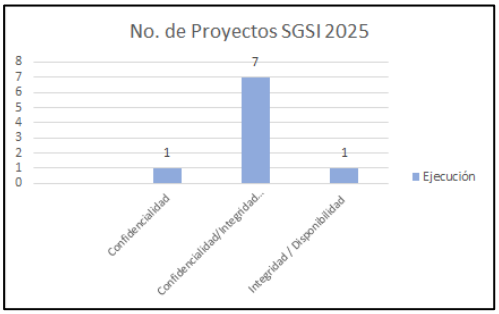
| No. | Principios SGSI | Política Asociada | Numeral Política - Resolución 3157 de 2021 | Acción o Proyecto Ejecutado | Objetivo | Fecha de Inicio | Fecha de Terminación | % de avance | Estado | Observaciones OCI |
|---|---|---|---|---|---|---|---|---|---|---|
| 8 | Confidencialidad/Integridad / Disponibilidad | Resolución 3157 de 2021 Artículo 2 - Política General del Sistema de Gestión de Seguridad de la Información | Artículo 6. Política de seguridad de los recursos humanos. | Realizar prácticas de Ingeniería social - Vishing (CID) | Objetivo Resolución 3157 de 2021: D. Promover, mantener y establecer la cultura de seguridad de la información en la Unidad para las Víctimas y partes interesadas. | 1/06/2025 | 31/10/2025 | 100% | Cerrado | Sin Observaciones |
| 9 | Confidencialidad/Integridad / Disponibilidad | Resolución 3157 de 2021 Artículo 2 - Política General del Sistema de Gestión de Seguridad de la Información | Artículo 6. Política de seguridad de los recursos humanos. Numeral 11 | Establecer el repositorio de información oficial del proceso o dependencia o DT en la herramienta SharePoint, que permita resguardar la información importante para la operación (CID) | Objetivo Resolución 3157 de 2021: 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 de la Entidad. | 1/05/2025 | 31/10/2025 | 100% | Cerrado | Sin Observaciones |

Fuente: OTI Tabla No. 1

### 5.2 Análisis de la Informacion Oficina de Control Interno

Como se puede observar en la anterior tabla, se evidencia una gestión de 9 proyectos que están asociados al cumplimiento a la implementación del Sistema de Gestión de Seguridad de la Información y a los planes de gestión que gobierna la Oficina de Tecnologías de la Información de la vigencia 2025.

| Principio SGSI | Ejecución |
|---|---|
| Confidencialidad | 1 |
| Confidencialidad/Integridad / Disponibilidad | 7 |
| Integridad / Disponibilidad | 1 |




Fuente: OTI Tabla y Grafico No. 2

Del análisis se concluye que la entidad presenta un nivel de cumplimiento operativo en la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), evidenciado en la ejecución del 100% de los proyectos definidos, todos en estado cerrado y alineados con los principios de confidencialidad, integridad y disponibilidad, conforme a lo establecido en la Resolución 3157 de 2021; sin embargo, dicho cumplimiento es predominantemente formal y operativo, y no necesariamente refleja un nivel adecuado de madurez ni de efectividad del sistema frente a los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC, la norma ISO/IEC 27001:2022 y el enfoque de control interno bajo MIPG, ni tampoco se tienen en cuenta las principales brechas que sean identificadas en el diagnostico en el proceso.

Si bien se evidencian avances importantes en la actualización de políticas, gestión de activos de información, ejecución de pruebas de continuidad, implementación de controles, prácticas de concientización y desarrollo de diagnósticos técnicos como la Declaración de Aplicabilidad (SOA), el SGSI presenta debilidades que limitan su consolidación como un sistema de gestión maduro. En particular, se identifica una orientación marcadamente reactiva, centrada en la operación y atención de incidentes, sin que se evidencie una integración efectiva del ciclo PHVA (Planear-Hacer-Verificar-Actuar), especialmente en las fases de verificación y mejora continua.

Desde la perspectiva de gestión de riesgos, aunque se reporta la identificación, valoración y tratamiento de riesgos de seguridad de la información, se observan inconsistencias en la actualización de matrices y ausencia de información en algunos procesos, lo que denota un cumplimiento parcial de los lineamientos del MSPI y de la cláusula 6.1 de ISO 27001, generando un riesgo asociado a la implementación de controles no alineados con el nivel real de exposición de la entidad. De igual forma, en la implementación de controles de seguridad, aunque se evidencia ejecución, no se identifica un análisis de brechas estructurado ni la definición de un roadmap de seguridad basado en criticidad, lo que sugiere una adopción de controles sin priorización técnica ni enfoque estratégico.

Uno de los aspectos críticos corresponde a la gestión de incidentes de seguridad de la información, donde, según lo evidenciado, el proceso se circunscribe a la atención y resolución de eventos, sin incorporar actividades como el análisis de causa raíz, la generación de lecciones aprendidas ni la definición de acciones de mejora, lo cual constituye una debilidad en la aplicación de la Resolución 3157 de 2021 y de los controles establecidos en ISO 27001, y limita la capacidad del SGSI para evolucionar y prevenir la recurrencia de incidentes.

En términos generales, el SGSI evaluado se ubica en un nivel de madurez intermedio, caracterizado por una implementación funcional de sus componentes, pero con debilidades en su articulación estratégica, medición, control y mejora continua. En consecuencia, aunque la entidad cumple formalmente con los requerimientos normativos, no se evidencia plenamente la eficacia del sistema para proteger los activos de información frente a amenazas reales, lo que implica la necesidad de fortalecer el enfoque basado en riesgos, consolidar el gobierno del SGSI, estructurar mecanismos de seguimiento y medición, y evolucionar

hacia un modelo de gestión proactivo, preventivo y orientado a la mejora continua, en concordancia con los estándares internacionales y las directrices del Gobierno Digital en Colombia.

**ANÁLISIS DEL COMPORTAMIENTO HISTORICO**.

**Ejecución Proyectos 2023-2024**

La Entidad en sus ultimas vigencias a ejecutado un total de 19 proyectos asociados a la implementación del SGSI de la Entidad de la siguiente manera:

| No. | Principios SGSI | Política Asociada | Acción o Proyecto Ejecutado | Objetivo | Año | Fecha de Inicio | Fecha de Terminación | % de avance | Estado |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Confidencialidad | Resolución 3157 de 2021<br>Artículo 8. Política de control de acceso. Esta política consiste en la identificación e implementación de controles que limiten el acceso a la información y a las instalaciones donde se procesa. | **Proyecto Ciberseguridad 360**<br><br>Aseguramiento de PCs<br><br>Control de acceso: Definir flujo de actividades para la gestión de usuarios; v. Documentar protocolo para la gestión de usuarios. (No oficialización) | Proteger la información y sistemas de información de la Unidad para la Atención y Reparación Integral de las Víctimas a partir de la implementación de las estrategias de seguridad digital definidas en este documento para las vigencias 2023-2026.<br><br>Objetivo Específico: Implementar los controles de seguridad de la información para mitigar, reducir o eliminar la divulgación, pérdida o modificación no controlada de los activos de la Entidad. | TR | 3/04/2023 | 30/06/2024 | 100% | Cerrado |
| 2 | Integridad / Disponibilidad | Resolución 3157 de 2021<br>Artículo 11. Política de seguridad de las operaciones. | **Proyecto Ciberseguridad 360**<br><br>Gestión de vulnerabilidades | Proteger la información y sistemas de información de la Unidad para la Atención y Reparación Integral de las Víctimas a partir de la implementación de las estrategias de seguridad digital definidas en este documento para las vigencias 2023-2026.<br><br>Objetivo Específico: Implementar los controles de seguridad de la información para mitigar, reducir o eliminar la divulgación, pérdida o modificación no controlada de los activos de la Entidad. | TR | 3/04/2023 | 30/06/2024 | 100% | Cerrado |

| No. | Principios SGSI | Política Asociada | Acción o Proyecto Ejecutado | Objetivo | Año | Fecha de Inicio | Fecha de Terminación | % de avance | Estado |
|---|---|---|---|---|---|---|---|---|---|
| 3 | Integridad / Disponibilidad | Resolución 3157 de 2021<br>Artículo 11. Política de seguridad de las operaciones. | **Proyecto Ciberseguridad 360**<br><br>Despliegue de licenciamiento de antivirus | Proteger la información y sistemas de información de la Unidad para la Atención y Reparación Integral de las Víctimas a partir de la implementación de las estrategias de seguridad digital definidas en este documento para las vigencias 2023-2026.<br><br>Objetivo Específico: Implementar los controles de seguridad de la información para mitigar, reducir o eliminar la divulgación, pérdida o modificación no controlada de los activos de la Entidad. | TR | 3/04/2023 | 30/06/2024 | 100% | Cerrado |
| 4 | Integridad / Disponibilidad | Resolución 3157 de 2021<br>Artículo 11. Política de seguridad de las operaciones. | **Proyecto SOC**<br><br>Adquisición e implementación Servicio del Centro de Operaciones de Seguridad | Implementar los servicios que proporcionará el SOC y transferirlos a la operación del dominio de seguridad de la información. | TR | 12/04/2024 | 31/12/2024 | 100% | Cerrado |
| 5 | Confidencialidad | Resolución 3157 de 2021<br>Artículo 8. Política de control de acceso. Esta política consiste en la identificación e implementación de controles que limiten el acceso a la información y a las instalaciones donde se procesa. | Acciones Adicionales<br><br>Implementación MFA<br><br>Acuerdo de Confidencialidad (plan SIG: 2023 y 2024 | Implementar los controles de seguridad y privacidad de la información para mitigar, reducir o eliminar la divulgación, pérdida o modificación no controlada de los activos de la entidad. | TR | Por Demanda | Por Demanda | NA | NA |
| 6 | Transversal (CDI) | Resolución 3157 de 2021 | Plan de Acción - PESI: Gestionar la actualización de los instrumentos de Gestión de la Información (Inventario de activos de Información, Índice de información clasificada y reservada y esquema de publicación | Implementar el Plan Estratégico de Seguridad de la información vigencia 2024 (PESI) | 2023 | 1/03/2023 | 31/12/2023 | 100% | Cumplida |
| 7 | Transversal (CDI) | Resolución 3157 de 2021 | Plan de Acción - PESI: Implementar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información Vigencia 2023 | Implementar el Plan Estratégico de Seguridad de la información vigencia 2024 (PESI) | 2023 | 1/05/2023 | 31/12/2023 | 100% | Cumplida |

| No. | Principios SGSI | Política Asociada | Acción o Proyecto Ejecutado | Objetivo | Año | Fecha de Inicio | Fecha de Terminación | % de avance | Estado |
|---|---|---|---|---|---|---|---|---|---|
| 8 | Transversal (CDI) | Resolución 3157 de 2021 | Plan de Acción - PESI: Actualizar la declaración de aplicabilidad de controles en la Entidad<br><br>Implementar los controles de seguridad aplicables al Proceso o DT, de acuerdo con la Declaración de aplicabilidad (SOA) | Implementar el Plan Estratégico de Seguridad de la información vigencia 2024 (PESI) | 2023 | 1/04/2023 | 31/12/2023 | 100% | Cumplida |
| 9 | Transversal (CDI) | Resolución 3157 de 2021 | Plan de Acción - PESI: Actualización (en caso de ser necesario) y socialización de políticas de seguridad de la información clasificadas por componente de aplicación (datos, aplicaciones, infraestructura, factor humano) | Implementar el Plan Estratégico de Seguridad de la información vigencia 2024 (PESI) | 2023 | 1/04/2023 | 31/12/2023 | 100% | Cumplida |
| 10 | Transversal (CDI) | Resolución 3157 de 2021 | Plan de Acción - PESI: Gestionar las actividades complementarias para el SGSI de la vigencia | Implementar el Plan Estratégico de Seguridad de la información vigencia 2024 (PESI) | 2023 | 1/04/2023 | 31/12/2023 | 100% | Cumplida |
| 11 | Transversal (CDI) | Resolución 3157 de 2021 | Plan de Acción - PESI: Fortalecer políticas de seguridad de la información a procesos, dependencias o líneas de trabajo | Implementar el Plan Estratégico de Seguridad de la información vigencia 2024 (PESI) | 2023 | 1/02/2023 | 31/12/2023 | 100% | Cumplida |
| 12 | Transversal (CDI) | Resolución 3157 de 2021 | Plan de Acción - PESI: Realizar seguimiento a la implementación del MSPI | Implementar el Plan Estratégico de Seguridad de la información vigencia 2024 (PESI) | 2023 | 1/04/2023 | 31/12/2023 | 100% | Cumplida |
| 13 | Transversal (CDI) | Resolución 3157 de 2021 | Plan de Acción - PESI: Realizar la atención y seguimiento a los eventos e incidentes de seguridad de la información | Implementar el Plan Estratégico de Seguridad de la información vigencia 2024 (PESI) | 2023 | 1/04/2023 | 31/12/2023 | 100% | Cumplida |
| 14 | Transversal (CDI) | Resolución 3157 de 2021 | Plan de Acción - PESI: Gestionar la identificación y clasificación de activos de información. | Implementar el Plan Estratégico de Seguridad de la información vigencia 2024 (PESI) | 2024 | 1/03/2024 | 31/10/2024 | 100% | Cumplida |
| 15 | Transversal (CDI) | Resolución 3157 de 2021 | Plan de Acción - PESI: Identificar, valorar, definir plan de tratamiento y realizar seguimiento de riesgos de activos críticos. | Implementar el Plan Estratégico de Seguridad de la información vigencia 2024 (PESI) | 2024 | 1/03/2024 | 31/12/2024 | 100% | Cumplida |
| 16 | Transversal (CDI) | Resolución 3157 de 2021 | Plan de Acción - PESI: Actualizar la Declaración de Aplicabilidad de controles en la Entidad. | Implementar el Plan Estratégico de Seguridad de la información vigencia 2024 (PESI) | 2024 | 1/06/2024 | 30/06/2024 | 100% | Cumplida |
| 17 | Transversal (CDI) | Resolución 3157 de 2021 | Plan de Acción - PESI: Implementar los controles de seguridad aplicables al Proceso o DT, de acuerdo con la Declaración de aplicabilidad (SOA) | Implementar el Plan Estratégico de Seguridad de la información vigencia 2024 (PESI) | 2024 | 1/07/2024 | 31/07/2024 | 100% | Cumplida |

| No. | Principios SGSI | Política Asociada | Acción o Proyecto Ejecutado | Objetivo | Año | Fecha de Inicio | Fecha de Terminación | % de avance | Estado |
|---|---|---|---|---|---|---|---|---|---|
| 18 | Transversal (CDI) | Resolución 3157 de 2021 | Plan de Acción - PESI: Implementar el Sistema de Gestión de Seguridad de la Información. (Alcance 2024) | Implementar el Plan Estratégico de Seguridad de la información vigencia 2024 (PESI) | 2024 | 1/02/2024 | 30/11/2024 | 100% | Cumplida |
| 19 | Transversal (CDI) | Resolución 3157 de 2021 | Plan de Acción - PESI: Plan de Cultura y Sensibilización en Seguridad de la Información. | Implementar el Plan Estratégico de Seguridad de la información vigencia 2024 (PESI) | 2024 | 1/03/2024 | 31/12/2024 | 100% | Cumplida |

Fuente: OTI Tabla No. 2

| Principios SGSI | Número de Proyectos Ejecutados | | | Total General |
|---|---|---|---|---|
| | 2023 | 2024 | TR[1] | |
| Confidencialidad | - | - | 2 | 2 |
| Integridad / Disponibilidad | - | 1 | 2 | 3 |
| Transversal | 8 | 6 | - | 14 |

Fuente: OTI Tabla No. 3

El análisis del comportamiento histórico del Sistema de Gestión de Seguridad de la Información (SGSI), basado en la información suministrada, evidencia un nivel sobresaliente de avance y cumplimiento en la ejecución de las acciones, proyectos y planes definidos. Se observa que la mayoría de las actividades han alcanzado un 100% de ejecución, encontrándose en estado “Cerrado” o “Cumplida”, lo que refleja una gestión consistente y orientada a resultados.

De igual manera, los resultados obtenidos en el marco de instrumentos estratégicos como el Plan Estratégico de Tecnologías de la Información (PESI) y las iniciativas de ciberseguridad asociadas, reflejan una articulación efectiva entre la planeación estratégica y la ejecución operativa, contribuyendo al fortalecimiento del enfoque preventivo, la mejora continua y la gestión adecuada de riesgos de seguridad de la información.

## 6. ENFOQUE BASADO EN RIESGOS.

[1] TR: Proyectos que se gestionaron y ejecutaron entre los años 2023 y 2024

Desde un enfoque basado en riesgos del Sistema de Gestión de Seguridad de la Información (SGSI), el análisis de la información evidencia que, si bien la entidad presenta un alto nivel de cumplimiento en la ejecución de actividades, es necesario fortalecer la orientación de la gestión hacia la identificación, tratamiento y monitoreo efectivo de los riesgos de seguridad de la información, más allá del cumplimiento operativo.

En este sentido, se identifica como riesgo principal la posibilidad de que el SGSI esté operando bajo un enfoque de cumplimiento formal, donde las actividades se ejecutan y se reportan como “cumplidas”, pero sin una validación suficiente de su efectividad en la mitigación de riesgos o que estén asociados a brechas identificadas en el sistema y clasificadas como críticas. Este escenario puede derivar en una percepción de seguridad eficiente, en la cual los controles existen documentalmente, pero no necesariamente reducen la probabilidad o el impacto de amenazas sobre los activos de información sin que existan indicadores que permitan una medición a través de la gestión de los resultados en las acciones planeadas.

Adicionalmente se identifica el riesgo de gestión inadecuada de incidentes de seguridad de la información, asociado a la ausencia de análisis de causa raíz, lecciones aprendidas y mecanismos de retroalimentación, lo que puede generar la repetición de incidentes, afectando la confidencialidad, integridad y disponibilidad de la información; este riesgo tiene como causa principal la debilidad en la fase de verificación del SGSI y como consecuencia la materialización recurrente de eventos de seguridad y pérdida de control institucional.

## 7. CONCLUSIONES DEL ANÁLISIS Y VALIDACIÓN DE EVIDENCIAS

Desde un enfoque de auditoría y madurez del SGSI, se identifican oportunidades de mejora relacionadas con la necesidad de fortalecer el análisis estratégico de las actividades ejecutadas, dado que, en varios casos, se evidencia un enfoque orientado al cumplimiento operativo, sin que se observe de manera consistente la incorporación de elementos clave como el análisis de causa raíz, la documentación de lecciones aprendidas o la evaluación de la efectividad de los controles implementados. Esta situación podría derivar en un riesgo de cumplimiento formal, en el cual se ejecutan las actividades planificadas, pero no necesariamente se garantiza la reducción efectiva de los riesgos de seguridad de la información.

En este contexto, se recomienda fortalecer el enfoque basado en riesgos, asegurando que cada actividad esté claramente vinculada a riesgos identificados y que incluya la evaluación de su impacto en la reducción de estos. Igualmente, se hace necesario incorporar mecanismos de medición de la efectividad de los controles, mediante la definición de indicadores de desempeño (KPIs) y de riesgo (KRIs), que permitan trascender del cumplimiento a la generación de valor. Se recomienda también estandarizar y mejorar la calidad de los registros y evidencias, implementar procesos formales de gestión de lecciones aprendidas,

así como fortalecer las auditorías internas del SGSI con un enfoque técnico que valide no solo la existencia de controles, sino su efectividad.

Finalmente, se sugiere continuar la alineación con buenas prácticas internacionales, tales como ISO/IEC 27001, ISO/IEC 27005 y el NIST Cybersecurity Framework, y avanzar hacia la adopción de modelos de madurez que permitan evolucionar el SGSI, desde un enfoque de cumplimiento hacia un modelo optimizado, orientado a la mejora continua, la gestión proactiva de riesgos y la resiliencia organizacional frente a amenazas de seguridad de la información.

**8. CONCEPTO DE CONTROL INTERNO**.

Del análisis efectuado, se evidencia que el SGSI presenta un nivel adecuado de diseño e implementación de controles, particularmente en lo relacionado con la planeación, ejecución y seguimiento de actividades, lo cual se refleja en altos porcentajes de cumplimiento y cierre de acciones. Lo anterior denota la existencia de controles de gestión (preventivos y detectivos) asociados al seguimiento de planes, así como mecanismos de monitoreo que permiten verificar el avance de las acciones definidas.

Sin embargo, desde una perspectiva de Control Interno, se identifican debilidades en la evaluación que se debe realizar a los controles definidos en los riesgos de seguridad de la información donde se identifique las principales brechas que como resultado estén calificadas como críticas y que deban ser abordadas y planificadas en la ejecución de acciones o actividades que permitan asegurar un avance sustantivo en la implementación del SGSI, dado que el énfasis actual se centra en el cumplimiento de actividades operativas, sin que se evidencie de manera consistente la aplicación de indicadores de resultado o mecanismos que permitan determinar si los controles implementados están mitigando los riesgos identificados dentro del SGSI. Esta situación limita la capacidad del sistema para asegurar razonablemente la protección de la confidencialidad, integridad y disponibilidad de la información.

En relación con el componente de evaluación del riesgo, se identifica que, aunque existen actividades asociadas al SGSI, no se evidencia una integración robusta entre la gestión de riesgos de seguridad de la información y la toma de decisiones, ni la utilización sistemática de indicadores clave de riesgo (KRIs) que permitan monitorear la exposición al riesgo y la eficacia de los controles en el tiempo, en concordancia con lo establecido por el DAFP y estándares como ISO/IEC 27005.

En conclusión, se evidencia que el SGSI se encuentra en proceso de implementación y operando de forma continua, con un adecuado nivel de cumplimiento en términos de ejecución; sin embargo, presenta situaciones en su efectividad y madurez, principalmente en la evaluación de controles, la integración del enfoque basado en riesgos y la medición de brechas que permita una madurez conforme a la criticidad que pueda identificarse en sus diferentes aspectos técnicos. Por lo anterior, se concluye que el sistema proporciona un nivel de seguridad razonable, pero susceptible de fortalecimiento, recomendándose la adopción de prácticas avanzadas, tales como la implementación de pruebas de efectividad de controles, definición de indicadores de riesgo y desempeño, fortalecimiento del monitoreo continuo, para lo cual las

buenas prácticas internacionales son una táctica importante como la alineación integral con marcos de referencia como COSO, ISO/IEC 27001 e ISO/IEC 27005, con el fin de consolidar un SGSI robusto, medible y orientado a la mejora continua.

**APROBÓ**

**JEFE DE OFICINA DE CONTROL INTERNO**

Elaborado: Basco Ricaurte Guerra Contratista Oficina de Control Interno