Fecha de Emisión del Informe	Día	21	Mes	07	Año	2025

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 a corte diciembre 31 del 2024.

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.

Este informe de seguimiento tiene como propósito 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 2024. El análisis se centra en los componentes clave del sistema: disponibilidad, confiabilidad e integridad de la información.

El informe está dirigido a la Dirección General, a los miembros del Comité Institucional de Control Interno, a la Oficina de Tecnologías de la Información y los usuarios de sistemas de información de la entidad. Son también son destinatarios los entes de control y a los ciudadanos en general que deseen hacer control social o realizar estudios académicos.

En el informe 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.

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 15 de abril se solicitó al líder de proceso de la Oficina de Tecnologías de la Informacion se indique cuáles han sido 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 lunes 05 de mayo a las 17:11 por parte del jefe de la Oficina de Tecnologías de la Información en donde indica:

> *“Por medio del presente me permito informar que se ha configurado el permiso de acceso de solo consulta a los proyectos que se gestionaron durante el 2023 y 2024, relacionados con la implementación del SGSI,*

teniendo en cuenta las Políticas y lineamientos de Seguridad de la Entidad". *PRY-0613031_Ciber-seguridad-360*

PRY-0614042_Estructuracion-SOC

"Adicionalmente, se remite adjunto el formato diligenciado donde se incluyeron los proyectos de Seguridad de la información (2023 y 2024) y sus principales componentes asociados a los principios de Confidencialidad, Integridad y Disponibilidad. Así mismo se relacionaron las acciones que se ejecutaron en el marco del PESI 2023 y 2024 relacionados de manera transversal con los principios. Adicionalmente, se relacionan las macro actividades que hicieron parte de los Planes Estratégicos de Seguridad de la Información, de las mencionadas vigencias, incluyendo los enlaces para el acceso a los correspondientes soportes"

Para finalizar, se asigna al Ingeniero Joaquín Rojas Palomino para la atención de las inquietudes que puedan surgir en el proceso de revisión.

5.1 Antecedentes

A la fecha de corte del seguimiento se presenta por parte de los responsables 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 las vigencias 2023 y 2024 relacionados de manera directa y transversal con los principios de seguridad de la información.

A continuación, se relacionan las acciones o proyectos ejecutados en las vigencias 2023 y 2024 teniendo en cuenta los principios de seguridad de la información de la siguiente manera:

No.	Principios SGSI	Política Asociada	Numeral Política	Acción o Proyecto Ejecutado	Objetivo	Fecha de Inicio	Fecha de Terminación	% de avance	Estado
1	Confidencialidad	Resolución 3157 de 2021 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.	ISO/IEC 27001:2013 A.9 Control de acceso ISO/IEC 27001:2022: 5.16 Gestión de la identidad 5.17 Información de autentificación 5.18 Derechos de acceso	**Proyecto Ciberseguridad 360** Aseguramiento de PCs 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. 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.	3/04/2023	30/06/2024	100%	Cerrado

No.	Principios SGSI	Política Asociada	Numeral Política	Acción o Proyecto Ejecutado	Objetivo	Fecha de Inicio	Fecha de Terminación	% de avance	Estado
2	Integridad / Disponibilidad	Resolución 3157 de 2021 Artículo 11. Política de seguridad de las operaciones.	ISO/IEC 27001:2013 A.12 Seguridad de las Operaciones ISO/IEC 27001:2022: 8.8 Gestión de las vulnerabilidades técnicas	**Proyecto Ciberseguridad 360** 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. 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.	3/04/2023	30/06/2024	100%	Cerrado
3	Integridad / Disponibilidad	Resolución 3157 de 2021 Artículo 11. Política de seguridad de las operaciones.	ISO/IEC 27001:2013 A.12 Seguridad de las Operaciones ISO/IEC 27001:2022: 8.7 Protección contra malware	**Proyecto Ciberseguridad 360** 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. 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.	3/04/2023	30/06/2024	100%	Cerrado
4	Integridad / Disponibilidad	Resolución 3157 de 2021 Artículo 11. Política de seguridad de las operaciones.	ISO/IEC 27001:2013 A.12 Seguridad de las Operaciones ISO/IEC 27001:2022: 8.7 Protección contra malware	**Proyecto SOC** 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.	12/04/2024	31/12/2024	100%	Cerrado

No.	Principios SGSI	Política Asociada	Numeral Política	Acción o Proyecto Ejecutado	Objetivo	Fecha de Inicio	Fecha de Terminación	% de avance	Estado
5	Confidencialidad	Resolución 3157 de 2021 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.	ISO/IEC 27001:2013 A.9 Control de acceso ISO/IEC 27001:2022: 5.16 Gestión de la identidad 5.17 Información de autentificación 5.18 Derechos de acceso	Acciones Adicionales Implementación MFA 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.	Por Demanda	Por Demanda	NA	NA
6	Transversal (CDI)	Resolución 3157 de 2021	ISO/IEC 27001:2013 ISO/IEC 27001:2022	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)	1/03/2023	31/12/2023	100%	Cumplida
7	Transversal (CDI)	Resolución 3157 de 2021	ISO/IEC 27001:2013 ISO/IEC 27001:2022	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)	1/05/2023	31/12/2023	100%	Cumplida
8	Transversal (CDI)	Resolución 3157 de 2021	ISO/IEC 27001:2013 ISO/IEC 27001:2022	Plan de Acción - PESI: Actualizar la declaración de aplicabilidad de controles en la Entidad 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)	1/04/2023	31/12/2023	100%	Cumplida
9	Transversal (CDI)	Resolución 3157 de 2021	ISO/IEC 27001:2013 ISO/IEC 27001:2022	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)	1/04/2023	31/12/2023	100%	Cumplida

No.	Principios SGSI	Política Asociada	Numeral Política	Acción o Proyecto Ejecutado	Objetivo	Fecha de Inicio	Fecha de Terminación	% de avance	Estado
10	Transversal (CDI)	Resolución 3157 de 2021	ISO/IEC 27001:2013 ISO/IEC 27001:2022	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)	1/04/2023	31/12/2023	100%	Cumplida
11	Transversal (CDI)	Resolución 3157 de 2021	ISO/IEC 27001:2013 ISO/IEC 27001:2022	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)	1/02/2023	31/12/2023	100%	Cumplida
12	Transversal (CDI)	Resolución 3157 de 2021	ISO/IEC 27001:2013 ISO/IEC 27001:2022	Plan de Acción - PESI: Realizar seguimiento a la implementación del MSPI	Implementar el Plan Estratégico de Seguridad de la información vigencia 2024 (PESI)	1/04/2023	31/12/2023	100%	Cumplida
13	Transversal (CDI)	Resolución 3157 de 2021	ISO/IEC 27001:2013 ISO/IEC 27001:2022	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)	1/04/2023	31/12/2023	100%	Cumplida
14	Transversal (CDI)	Resolución 3157 de 2021	ISO/IEC 27001:2013 ISO/IEC 27001:2022	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)	1/03/2024	31/10/2024	100%	Cumplida
15	Transversal (CDI)	Resolución 3157 de 2021	ISO/IEC 27001:2013 ISO/IEC 27001:2022	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)	1/03/2024	31/12/2024	100%	Cumplida
16	Transversal (CDI)	Resolución 3157 de 2021	ISO/IEC 27001:2013 ISO/IEC 27001:2022	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)	1/06/2024	30/06/2024	100%	Cumplida

No.	Principios SGSI	Política Asociada	Numeral Política	Acción o Proyecto Ejecutado	Objetivo	Fecha de Inicio	Fecha de Terminación	% de avance	Estado
17	Transversal (CDI)	Resolución 3157 de 2021	ISO/IEC 27001:2013 ISO/IEC 27001:2022	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)	1/07/2024	31/07/2024	100%	Cumplida
18	Transversal (CDI)	Resolución 3157 de 2021	ISO/IEC 27001:2013 ISO/IEC 27001:2022	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)	1/02/2024	30/11/2024	100%	Cumplida
19	Transversal (CDI)	Resolución 3157 de 2021	ISO/IEC 27001:2013 ISO/IEC 27001:2022	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)	1/03/2024	31/12/2024	100%	Cumplida

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 19 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 las vigencias 2023 y 2024.

Principio SGSI	Proyectos o Acciones	Ejecución		
		2023	2023 -2024	2024
Confidencialidad	2	-	1	-
Integridad -Disponibilidad	3	-	2	1
Transversal (CDI)	14	8	-	6

Fuente: OTI Tabla No. 2

Respecto al principio de confidencialidad, una de las acciones o proyectos reportados hace referencia a los acuerdos de confidencialidad, los cuales están caracterizados por ser ejecutados por demanda. Por esta razón, no es posible realizar una medición de su gestión durante las vigencias 2023 o 2024.

Ante esto, se recomienda que este tipo de acciones se realicen con una periodicidad anual, preferiblemente al inicio de cada vigencia, renovando los acuerdos de confidencialidad según las necesidades de los procesos. Adicionalmente, dichos acuerdos deberán renovarse siempre que sea necesario para dar

cumplimiento a obligaciones adquiridas ya sea por parte de funcionarios o contratistas que requieran nuevos accesos a la infraestructura tecnológica o a los sistemas de información de la Entidad.

Ejecución de los Proyectos 2024

De acuerdo con la información proporcionada por la Oficina de Tecnologías de la Información, durante la vigencia 2024 se ejecutaron directamente seis (6) proyectos, es decir, que iniciaron y finalizaron en el mismo año. Adicionalmente, se culminaron proyectos que habían comenzado en 2023 y concluyeron su ejecución en 2024, sumando un total de once (11) proyectos ejecutados.

Con base en lo anteriormente indicado, la Oficina de Control Interno procedió a evaluar la información recibida, concluyendo que los proyectos planeados fueron ejecutados en su totalidad. No obstante, se considera necesario tener en cuenta una serie de recomendaciones orientadas a la implementación de indicadores de gestión y a la generación de documentación técnica que permita evidenciar los avances, el cierre de brechas y el cumplimiento de los objetivos. Esto contribuirá a obtener resultados evolutivos y a generar nuevas acciones encaminadas al mejoramiento continuo para nuevas vigencias.

No.	Principios SGSI	Acción o Proyecto Ejecutado	Recomendación OCI
1	Confidencialidad	**Proyecto Ciberseguridad 360** Aseguramiento de PCs Control de acceso: Definir flujo de actividades para la gestión de usuarios; v. Documentar protocolo para la gestión de usuarios. (No oficialización)	Es indispensable establecer indicadores de gestión que permitan identificar con precisión las brechas y avances obtenidos durante la ejecución del proyecto. Asimismo, se requiere la incorporación de documentación técnica que respalde una evaluación sistemática y continua del cumplimiento de los objetivos y del progreso alcanzado.
2	Integridad / Disponibilidad	**Proyecto Ciberseguridad 360** Gestión de vulnerabilidades	Implementación de documentación técnica que permita realizar un seguimiento y control efectivo de la gestión aplicada a las remediaciones ejecutadas de acuerdo con el nivel de criticidad de las vulnerabilidades identificadas.
3	Integridad / Disponibilidad	**Proyecto Ciberseguridad 360** Despliegue de licenciamiento de antivirus	Implementación de documentación técnica que permita evidenciar la aplicación progresiva de políticas o parametrizaciones efectuadas en la herramienta, asegurando su estabilización de forma eficiente y continua.
4	Integridad / Disponibilidad	**Proyecto SOC** Adquisición e implementación Servicio del Centro de Operaciones de Seguridad	Implementación de documentación técnica que permita evidenciar el proceso realizado a la implementación del SOC, así como también su administración uso y manejo.
5	Confidencialidad	Acciones Adicionales Implementación MFA Acuerdo de Confidencialidad (plan SIG: 2023 y 2024	Definición especifica de la política de seguridad de la información que indica la elaboración de los acuerdos de confidencialidad en cuanto a los momentos y tiempos que se debe gestionar esta documentación, definiendo periodicidades según las necesidades de la Entidad.
6	Transversal (CDI)	Plan de Acción - PESI: Gestionar la identificación y clasificación de activos de información.	Inclusión de acciones encaminadas al conocimiento permanente sobre los activos de información de cada uno de los procesos que gestiona la Entidad.

No.	Principios SGSI	Acción o Proyecto Ejecutado	Recomendación OCI
7	Transversal (CDI)	Plan de Acción - PESI: Identificar, valorar, definir plan de tratamiento y realizar seguimiento de riesgos de activos críticos.	Implementación de indicadores que permitan una evaluación del cumplimiento de los controles de los riesgos asociados a los procesos.
8	Transversal (CDI)	Plan de Acción - PESI: Actualizar la Declaración de Aplicabilidad de controles en la Entidad.	Implementación de documentación técnica que permita evidenciar los avances realizados por los procesos al cumplimiento de la normativa.
9	Transversal (CDI)	Plan de Acción - PESI: Implementar los controles de seguridad aplicables al Proceso o DT, de acuerdo con la Declaración de aplicabilidad (SOA)	Implementación de documentación técnica que permita evidenciar los avances realizados por los procesos al cumplimiento de la normativa.
10	Transversal (CDI)	Plan de Acción - PESI: Implementar el Sistema de Gestión de Seguridad de la Información. (Alcance 2024)	Falta de control de la documentación técnica que permita evidenciar los propósitos de la ejecución de las acciones alineadas a los planes de seguridad de la información.
11	Transversal (CDI)	Plan de Acción - PESI: Plan de Cultura y Sensibilización en Seguridad de la Información.	Falta de control de la documentación técnica que permita evidenciar los resultados de los planes propuestos y la metodología con la que se diseña la identificación de las principales brechas sobre seguridad de la información.

Fuente: OTI Tabla No. 3

ANÁLISIS DEL COMPORTAMIENTO HISTORICO.

Conforme a la información entregada por la Oficina de Tecnologías de la Información para la vigencia 2023, se describen ocho (8) proyectos ejecutados en un 100%, donde se incluyen de manera transversal los principios del SGSI, sin embargo en la evaluación de seguimiento efectuado por la Oficina de Control Interno, se evidencia una serie recomendaciones a la ejecución de los proyectos en donde es necesario incluir documentación o indicadores de resultados que permitan evidenciar de manera eficiente el cumplimiento de los objetivos y el avance determinado en cada uno de los compromisos adquiridos en los planes respectivos de la siguiente manera:

Proyectos 2023

No.	Principios SGSI	Acción o Proyecto Ejecutado	Recomendación OCI
1	Transversal (CDI)	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	No se especifica las acciones que impactaron directamente en los planes de gestión y cuáles fueron las brechas identificadas en seguridad de la información que se redujeron a la ejecución de las actividades.

No.	Principios SGSI	Acción o Proyecto Ejecutado	Recomendación OCI
2	Transversal (CDI)	Plan de Acción - PESI: Implementar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información Vigencia 2023	Implementación de indicadores que permitan una evaluación del cumplimiento de los controles de los riesgos asociados a los procesos.
3	Transversal (CDI)	Plan de Acción - PESI: Actualizar la declaración de aplicabilidad de controles en la Entidad. Implementar los controles de seguridad aplicables al Proceso o DT, de acuerdo con la Declaración de aplicabilidad (SOA)	Implementación de documentación técnica que permita evidenciar los avances que han realizado los procesos al cumplimiento de la normativa.
4	Transversal (CDI)	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)	No se evidencia el resultado del ejercicio de la evaluación de la actualización de las políticas de Seguridad de la Información ni la metodología utilizada según los aspectos evolutivos en la gestión de datos que son utilizados por la Entidad.
5	Transversal (CDI)	Plan de Acción - PESI: Gestionar las actividades complementarias para el SGSI de la vigencia	No se especifica las acciones que impactaron directamente en los planes de gestión y que redujeron las brechas identificadas en seguridad de la información con este tipo de proyectos ejecutados
6	Transversal (CDI)	Plan de Acción - PESI: Fortalecer políticas de seguridad de la información a procesos, dependencias o líneas de trabajo	No se evidencia los análisis previos y posteriores sobre los impactos que ejercen este tipo de acciones para la evolución de los planes respectivos y más aún sobre el sistema de gestión de seguridad de la Información.
7	Transversal (CDI)	Plan de Acción - PESI: Realizar seguimiento a la implementación del MSPI	No se incluye los análisis sobre los resultados del MSPI según su actualización, es importante implementar informes de gestión que permitan la identificación de las principales brechas en los indicadores de los instrumentos de seguimiento y control y la configuración de los planes de acción respectivos según las metas propuestas o identificadas.
8	Transversal (CDI)	Plan de Acción - PESI: Realizar la atención y seguimiento a los eventos e incidentes de seguridad de la información	En los informes no se incluye análisis de los incidentes que permitan a la Entidad un mejoramiento continuo de este tipo de casos, en donde las remediaciones implementadas se enfoquen a la inclusión de políticas o parametrización de las herramientas con la que cuenta la entidad para la mitigación de situaciones que afecten la seguridad de la información.

Fuente: OTI Tabla No. 4

6. ENFOQUE BASADO EN RIESGOS.

La Oficina de Control interno, luego de revisar los soportes aportados por la dependencia responsable de la implementación de las actividades descritas en los diferentes planes asociadas al Sistema de Gestión

de Seguridad de la Información evidencia los posibles riesgos que puede estar abocada la Entidad en lo que respecta a seguridad de la Información de la siguiente manera:

1. Posibilidad de Perdida de económica y reputacional por perdida a la Integridad y Disponibilidad de la Información de la Entidad, debido a la falla o la ausencia de controles para la remediación de vulnerabilidades identificadas en la infraestructura tecnológica de la Entidad y/o materialización de incidentes de seguridad.

2. Posibilidad de pérdida reputacional ante nuestras partes interesadas por falta de disponibilidad y mal uso de los activos de información críticos de los procesos, debido a la falta de apropiación de las políticas y lineamientos de seguridad de la información.

3. Posibilidad de pérdida económica y reputacional por perdida de la confidencialidad de la información de la Entidad debido a la falla o ausencia de controles relacionados con el acceso a información clasificada o reservada.

4. Posibilidad de pérdida económica y reputacional por perdida de la Disponibilidad de la información de la Entidad debido a la falla o ausencia de controles de seguridad aplicables

5. Posibilidad de pérdida económica y reputacional por perdida de la Confidencialidad, Integridad y Disponibilidad de la información registrada en documentos físicos, digitales y/o sistemas de información, por el acceso no controlado a la información sensible o confidencial y el desconocimiento de los lineamientos de seguridad de la información de la Entidad.

6. Riesgo fiscal, dado que los recursos aplicados a los sistemas de información no puedan dar los resultados esperados relacionados con la interoperabilidad de los sistemas, lo que puede implicar una actividad antieconómica.

7. CONCLUSIONES DEL ANÁLISIS Y VALIDACIÓN DE EVIDENCIAS

De acuerdo con los análisis y evaluaciones realizados por la Oficina de Control Interno, se evidencia la ausencia de controles e indicadores de gestión que permitan hacer seguimiento a las actividades ejecutadas para mitigar los riesgos y brechas identificadas en relación con el cumplimiento de las regulaciones y buenas prácticas del Sistema de Gestión de Seguridad de la Información de la Entidad y de las estrategias propuestas, tampoco se evidencia documentación técnica que permita demostrar que el modelo implementado se ha cumplido en sus diferentes fases.

8. CONCEPTO DE CONTROL INTERNO.

La gestión de la seguridad de la información se articula mediante procesos, procedimientos y políticas que forman parte del Sistema de Gestión de la Calidad que en este caso es el Sistema de Gestión de Seguridad

de la Información SGSI. Esta integración facilita la trazabilidad, control y mejora continua de los mecanismos de protección de datos. Además, garantiza que el tratamiento de la información, en sus distintas dimensiones (confidencialidad, integridad y disponibilidad), se ajuste a los marcos regulatorios vigentes, reduciendo la probabilidad de incidentes de seguridad y asegurando la protección de los datos frente a actores internos y externos.

A partir del análisis de las evidencias y soportes aportados por el proceso responsable, la Oficina de Control Interno concluye que no es posible determinar de manera precisa los avances en la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) respecto a las dimensiones evaluadas: disponibilidad, confidencialidad e integridad. Tampoco se puede establecer el comportamiento de los principales objetivos definidos en los planes de gestión formulados por el proceso responsable en cuanto al cierre de brechas identificadas. Esta limitación se debe a la ausencia de indicadores de gestión y la falta de informes de seguimiento que permita a los lectores determinar la ejecución de las actividades alineadas con las estrategias de seguridad de la información, los cuales son necesarios para evidenciar los avances logrados o identificar las situaciones que han dificultado el cumplimiento de los objetivos y alcances establecidos.

La Oficina de Control Interno recomienda la implementación de herramientas o instrumentos internos que permitan fortalecer la evaluación y el avance de las actividades y objetivos establecidos, en concordancia con las metas definidas. Asimismo, sugiere la inclusión de informes de seguimiento que evidencien el proceso de mejoramiento continuo tanto de las estrategias adoptadas en materia de seguridad de la información como del modelo de gestión propuesto, con el fin de facilitar la planificación de actividades y acciones futuras.

APROBÓ

JEFE DE 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.