N° DE INFORME	**4.3.1**
TIPO DE INFORME	**Evaluación de los riesgos y controles de Tecnologías de la Información**
PROCESO	**CP-TI-03. V1 Proceso Tecnologías de la Información**
RESPONSABLES	**Jefe Oficina de Tecnologías de la Información**
EQUIPO AUDITOR	
Marisol Gutierrez Hernandez	

1. OBJETIVO GENERAL

Evaluar el diseño y ejecución de los controles de Seguridad Digital, así como su pertinencia de acuerdo a los riesgos identificados en la Matriz de Riesgos de Seguridad de la Información.

2. OBJETIVOS ESPECÍFICOS

1. Verificar el diseño y ejecución de los controles a partir de los criterios definidos en la metodología y a partir de ello determinar si son adecuados para evitar la materialización de riesgos.
2. Verificar que se realice seguimiento a la ejecución de los controles y acciones del plan de manejo de riesgos y el estado de acuerdo a los soportes.

3. ALCANCE

La evaluación tiene como alcance la revisión de controles del Mapas de Riesgos de Seguridad de la Información de la vigencia 2025 al corte de Septiembre de 2025.

4. CRITERIOS (NORMATIVIDAD)

- Ley 87 de 1993, artículo 12. Funciones de los auditores internos. c) Verificar que los controles definidos para los procesos y actividades de la organización, se cumplan por los responsables de su ejecución y en especial, que las áreas o empleados encargados de la aplicación del régimen disciplinario ejerzan adecuadamente esta función; d) Verificar que los controles asociados con todas y cada una de las actividades de la organización estén adecuadamente definidos, sean apropiados y se mejoren permanentemente, de acuerdo con la evolución de la entidad; d). Verificar que los controles asociados con todas y cada una de las actividades de la organización, estén adecuadamente definidos, sean apropiados y se mejoren permanentemente, de acuerdo con la evolución de la entidad; g. Verificar los procesos relacionados con el manejo de los recursos, bienes y los sistemas de información de la entidad y recomendar los correctivos que sean necesarios.
- Decreto 648 de 2017, artículo 2.2.21.3.1. “El Sistema Institucional de Control Interno estará integrado por el esquema de controles de la organización, la gestión de riesgos, la administración de la información y de los recursos y por el conjunto de planes, métodos, principios, normas, procedimientos, y mecanismos de verificación y evaluación adoptados por la entidad, dentro de las políticas trazadas por la dirección y en atención a las metas, resultados u objetivos de la entidad.”
- Guía Rol de las Unidades de Control Interno, Auditoría Interna o quien haga sus veces. DAFP. 2023.
- Guía administración del riesgo y el diseño de controles en entidades públicas V6. DAFP. 2022. “…a fin de facilitar la estructura para los seguimientos y monitoreos en todos los niveles organizacionales, actividades o acciones propias de cada línea así: … *la 1ª línea de defensa todos los servidores tienen una responsabilidad frente a la aplicación efectiva de los controles, por lo que se trata de un seguimiento permanente, esto incluye la aplicación de controles de gerencia operativa que corresponde a aquellos que son aplicados por servidores con personal”… a cargo la 3ª línea de defensa que corresponde a la Oficina de Control Interno o quien hace sus veces, a través de sus procesos de seguimiento y evaluación…”. “…Tratamiento del riesgo – rol de la primera línea de defensa: Como medio para propiciar el logro de los objetivos, las actividades de control se orientan a*

prevenir y detectar la materialización de los riesgos. Por consiguiente, su efectividad depende de qué tanto se están logrando los objetivos estratégicos y de proceso de la entidad. Le corresponde a la primera línea de defensa el establecimiento de actividades de control" (pag.92).

- Mapas de Riesgos de Seguridad Digital ART 2025
- MI-TI-01 V5 Manual de Políticas de Seguridad de la Información Numeral 6. POLÍTICAS ORGANIZACIONALES -6.1. ROLES Y RESPONSABILIDADES; Numeral 48. POLÍTICA DE REVISIONES DE SEGURIDAD DE LA INFORMACIÓN
- POL-DE-08 V1 Manual de Política de Administración del Riesgo 2024. Numeral 9.1. Monitoreo de los riesgos y controles. 9.2 Seguimiento a los mapas de riesgos.

5. PERSONAL ENTREVISTADO

Juan Jose Sanchez Rodriguez, Deysi Viviana Gómez; Contratistas OTI
Freddy Alejandro Aguas Barbosa – Jefe OTI

6. METODOLOGÍA

Se informó mediante Memorando 20251010071413 del 18 de septiembre del 2025 la ejecución del informe correspondiente a la evaluación de riesgos y controles de Seguridad de la Información vigencia 2025; En reuniones programadas con los delegados, se revisaron: la Matriz de riesgos de Seguridad de la Información vigente y el Seguimiento a las acciones correspondientes al Plan de Manejo de Riesgos de Seguridad de la Información, en las cuales se revisaron y verificaron las actividades de control y acciones establecidas así como su ejecución y validación de evidencias que fueron aportadas en un repositorio de OneDrive al cual se dio acceso Riesgos 2025

Con el fin de realizar la evaluación a los controles determinados en el Mapa de Riesgos de Seguridad de la Información, se determinaron como criterios y metodología para evaluar el diseño y ejecución de los controles los siguientes:

Tabla N°1:

[1]Criterio por evaluar	Factor por evaluar	Puntaje	Puntaje
Asignación y segregación del responsable	Responsable asignado Existe segregación en las actividades de control No se identifica responsable	10 5 0	15
Periodicidad o Frecuencia[2]	Se describe la periodicidad y en la ejecución es Oportuna y continua Se ejecuta, pero no es claro cuando No describe periodicidad.	15 10 0	15
Propósito[3] – Acción de la Actividad de Control	Se describe la acción de acuerdo con un verbo indicativo de control y de acuerdo con lo determinado (Preventivo o Detectivo). Se observa el propósito, pero tiene debilidades en su redacción. No es claro el propósito / No es un control (corresponde a actividades, pero no de control, de acuerdo con el verbo utilizado o actividad desarrollada)	15 10 0	15

[1] Aspectos por evaluar dentro del Sistema de Control Interno - Manual Operativo MIPG. Pág. 126
[2] Atributos informativos (Guía de Administración de Riesgos del DAFP) – Frecuencia.
[3] Para qué se realiza el control, o que se debe: Verificar, validar, conciliar, comparar, revisar, cotejar, detectar, etc. Permite evaluar si la fuente u origen de la información que sirve para ejecutar el control es confiable para la mitigación del riesgo

[4]Ejecución de la Actividad de Control	Se describe y ejecuta claramente Se describe o ejecuta de manera incompleta de acuerdo con lo observado y presentado en la revisión y/o las evidencias no corresponden a la ejecución del complemento. No es clara la descripción del complemento o no se ejecuta.	15 10 0	15
Análisis de Desviaciones[5]	Se describen y resuelven Ejecutadas sin evidencia No determinadas o ejecutadas	15 10 0	15
[6]Evidencia de Ejecución del Control	Completa (evidencia de Propósito, Complemento y desviaciones) Incompleta No Existe	15 10 0	15
Coherencia con el Riesgo	SI NO	5 0	5
[7]Soportado en Procedimientos Manuales o políticas del SIG	SI NO	5 0	5

Fuente: Elaboración propia - Grupo interno de trabajo de Control Interno – GITCI, con base en la Guía de Administración de Riesgos del DAFP.

De acuerdo a los resultados de la revisión en mesas de trabajo y de acuerdo a las evidencias presentadas por los delegados y los criterios determinados por el Auditor del GITCI, se realizó la valoración y evaluación cuantitativa y cualitativa en el papel de trabajo con el fin de establecer si los controles cumplen los lineamientos en cuanto al diseño y ejecución, de esta manera el determinar si los controles existentes son adecuados para evitar la materialización de riesgos.

De acuerdo con los resultados cuantitativos para cada criterio evaluado, se generó una calificación o resultado cualitativo de la evaluación del diseño y ejecución de los controles así:

Tabla N°2:

Escala de valoración- Nivel de madurez de los controles en cuanto a diseño y ejecución			
OPTIMO	**5**	**95- 100**	Los controles permitieron prevenir la materialización del riesgo, están definidos de manera adecuada de conformidad con lo estipulado en la Guía del DAFP y MIPG en cuanto al diseño y ejecución, son coherentes con el objetivo del proceso, se soportan en procedimientos y/o políticas actualizadas y se tiene evidencia de su ejecución y registro de desviaciones.
SATISFACTORIO	**4**	**90-94**	En este nivel el control: Aunque el control permite prevenir la materialización del riesgo, presenta observaciones para la mejora; o, Se encuentra bien diseñado y se ejecuta de manera conforme sin embargo se materializó el riesgo.
ADECUADO	**3**	**80-89**	En este nivel el control: Presenta debilidades y amerita una mejora en su diseño o ejecución.
REGULAR	**2**	**50-79**	En este nivel el control: Presenta debilidades importantes por lo que se requiere replantear. Debilidades en cuanto a: diseño y ejecución (no documentado adecuadamente o sin evidencias conforme a su ejecución). No previene la materialización de riesgo, o que, estando adecuadamente definido, no se ejecuta por parte del(os) responsable(s) directo(s).
DEFICIENTE	**1**	**0-45**	No cumple con los criterios para que sea un control efectivo en su diseño y ejecución.

Fuente: Elaboración propia equipo Grupo interno de trabajo de Control Interno – GITCI.

[4] Se refiere al "Complemento" descrito en la Guía de Administración de Riesgos del DAFP en la cual se define a través de que medio o herramienta de control se ejecuta la "Acción" (como lo hace el responsable).
[5] Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control. Si el responsable de ejecutar el control no realiza ninguna actividad de seguimiento a las observaciones o desviaciones, o la actividad continúa a pesar de indicar esas observaciones o desviaciones, el control tendría problemas de diseño.
[6] Atributos informativos (Guía de Administración de Riesgos del DAFP) – Evidencia.
[7] Atributos informativos (Guía de Administración de Riesgos del DAFP) – Documentación.

7. DESARROLLO

7.1 Objetivo 1: Verificar el diseño y ejecución de los controles a partir de los criterios definidos en la metodología y a partir de ello determinar si son adecuados para evitar la materialización de riesgos.
De la herramienta de evaluación (Papel de trabajo) se extrae el siguiente resultado, el detalle de evaluación de cada uno de los controles de acuerdo a los criterios se presenta como anexo:

Tabla N° 3. Solidez del conjunto de controles del Mapa de Riesgos de Seguridad de la Información

Numero de Riesgo	Evaluación Controles	Valoración
Riesgo 1	**95**	OPTIMO
Riesgo 2	**95**	OPTIMO
Riesgo 3	**70**	REGULAR
Riesgo 4	**80**	ADECUADO
Riesgo 5	**100**	OPTIMO
Riesgo 6	**60**	REGULAR
Riesgo 7	**95**	OPTIMO
Riesgo 8	**100**	OPTIMO
Riesgo 9	**80**	ADECUADO
Riesgo 10	**100**	OPTIMO
Riesgo 11	**100**	OPTIMO
Riesgo 12	**100**	OPTIMO
Riesgo 13	**100**	OPTIMO
Riesgo 14	**50**	REGULAR
Riesgo 15	**100**	OPTIMO
Riesgo 16	**95**	OPTIMO
Riesgo 17	**100**	OPTIMO
Riesgo 18	**100**	OPTIMO
Consolidado promedio	**90**	SATISFACTORIO

Fuente: Papel de trabajo evaluación riesgos SI

De lo anterior se concluye que de los 18 riesgos identificados a partir de los activos de información reportados por los responsables en 1ª línea de defensa, se establecieron 18 controles y 18 actividades de plan de manejo de los riesgos, encontrando que 13 controles se encuentran en nivel “Optimo” respecto a su diseño y ejecución calificados en promedio con 98 puntos, 2 controles valorados en un nivel “Adecuado” con 80 puntos y sobre los cuales se deben generar mejoras en su diseño, 3 en nivel “Regular” que ameritan correcciones y ajustes en cuanto a diseño y ejecución especialmente en la definición de responsables y evidencias, y 3 en un Nivel “Deficiente” debido a que como están descritos no corresponden a las características de diseño de controles efectivos. En promedio los controles de Seguridad de la Información se encuentran en un nivel **SATISFACTORIO** con ocasión a que el 72% de los mismos se encuentran en el más alto nivel (OPTIMO) y el 28% requieren mejoras en diseño y ejecución.

7.2 Objetivo 2: Verificar que se realice seguimiento a la ejecución de los controles y acciones del plan de manejo de riesgos y el estado de acuerdo a los soportes.

De acuerdo a las evidencias aportadas y la evaluación cuantitativa, a continuación, se describen las situaciones encontradas en las observaciones frente a cada uno de los controles y acciones del Plan de manejo así:

Tabla N° 4. Resultados de Evaluación de Controles y Acciones

N.	RIESGO	Controles	Acciones Plan de Manejo	Estado Acciones Plan de Manejo	Observaciones frente al diseño y ejecución del Control y acciones del Plan de Manejo (Según Evidencias)
1	Posibilidad de afectación reputacional y económico por acceso no autorizado o alteración de la información, generando pérdida de confidencialidad, integridad y disponibilidad de la información, debido a las vulnerabilidades del repositorio.	Cada vez que se realice una solicitud de acceso por cada dependencia, el responsable de la mesa de servicio, verifica: El Diligenciamiento de formato de control de acceso(FM-TI-07.V7 Formato de control de accesos). Con el fin de Remitirlo al área de SI para su aprobación y proceder a conceder los permisos a los usuarios. En caso de encontrar que el formato no se encuentre debidamente diligenciado se devuelve al peticionario a través del caso de la mesa de servicio. Evidencias formatos de control de acceso firmados mes a mes durante el periodo.	Se verifica semestralmente que no tengan acceso funcionarios y/o contratistas a los repositorios cuando ya se han desvinculado.	Indeterminado	Se observa con la descripción del control que se cumplen los criterios, sin embargo, es pertinente incluir como soporte del control, los correos enviados en caso de encontrar desviaciones de acuerdo a lo descrito. No porque no se tengan sino porque no se aportaron en la carpeta de evidencias y no se refieren en la columna de evidencias. Respecto al Plan de Manejo de Riesgos, se debe contar con una evidencia que permita identificar los resultados del seguimiento realizado (muestra verificada, fecha, entre otros) que determine si efectivamente los funcionarios/contratistas desvinculados a la ART no tienen acceso a los repositorios.
2	Posibilidad de afectación reputacional por deterioro de la información, generando pérdida de integridad y disponibilidad de la información, debido a las vulnerabilidades del repositorio.	Cada vez que una dependencia requiere consultar o extraer información física (por ejemplo, carpetas de contratos, expedientes o soportes contables), el responsable del Archivo Central realiza el siguiente procedimiento: El funcionario solicitante envía una petición formal por correo institucional a través del formato (FM-GA-10. V7 Solicitud Préstamo y Devolución de expedientes). El responsable del repositorio verifica la validez y pertinencia de la solicitud antes de permitir el acceso al área o la entrega del documento. El funcionario realiza la revisión del material. Al finalizar, el custodio verifica la devolución completa de los documentos y registra el cierre del acceso en la bitácora.	Se verifica mensualmente por parte del profesional encargado del archivo central que los documentos prestados a funcionarios y/o contratistas se encuentren alojados en los repositorios cuando haya finalizado el préstamo.	En Ejecución con debilidades en evidencias	Se observa con la descripción del control que se cumplen los criterios; Se observa entre las evidencias archivo Excel "PRESTAMO Y CONSULTA DE EXPEDIENTES AÑO 2025" con corte al mes de agosto de 2025 aunque no se menciona en la actividad de control sino en la columna de evidencias como Mecanismo de alerta de para devolución; se sugiere incluirse uso en la actividad de control considerando que con esta herramienta posteriormente se controla la entrega de los documentos de archivo en préstamo; Se sugiere ajustar en cuanto a ello y puntualizar en las desviaciones y acciones en caso de presentarse, así como la evidencia que se genera. Respecto al Plan de Manejo de Riesgos, se aportan como evidencia formatos de préstamo y no los resultados de la verificación mensual que se planteó. Se sugiere revisar y ajustar debido a que las evidencias aportadas no son consistentes con la acción del Plan de Manejo.

N.	RIESGO	Controles	Acciones Plan de Manejo	Estado Acciones Plan de Manejo	Observaciones frente al diseño y ejecución del Control y acciones del Plan de Manejo (Según Evidencias)
3	Posibilidad de afectación reputacional por acceso no autorizado o filtración de datos, generando pérdida de confidencialidad e integridad de la información, debido a las malas prácticas del uso de la cuenta de correo	Restringir y gestionar el acceso al buzón de denuncias únicamente al personal designado y autorizado, mediante el diligenciamiento del Formato de Control de Acceso (FM-TI-07.V7). El encargado de infraestructura deberá configurar autenticación multifactor (MFA) y credenciales únicas para los responsables autorizados, garantizando que solo el personal aprobado pueda acceder al buzón. Ante cualquier incidente de seguridad o acceso no autorizado, se deberán ejecutar medidas correctivas inmediatas, incluyendo restablecimiento de credenciales, bloqueo de cuentas y notificación a las partes afectadas.	A la cuenta de correo de buzón de denuncias se le activa el (MFA), limitando el acceso exclusivamente al personal designado. Se realiza un monitoreo mensual por parte del SOC de los accesos para detectar intentos no autorizados o actividades sospechosas, aplicando medidas correctivas inmediatas cuando se identifiquen incidentes, tales como restablecimiento de credenciales, bloqueo de cuentas y notificación a las partes afectadas. Además, se revisará trimestralmente la efectividad de estas acciones	En Ejecución con debilidades en evidencias	La descripción de la actividad de control presenta debilidades en su redacción debido a que corresponde a una actividad de gestión realizada no de manera periódica sino eventual considerando que se presenta en las evidencias el formato de control de accesos cuando se asignó al usuario de la cuenta de correo, lo que corresponde a las causas (*por acceso no autorizado o filtración de datos*), pero no es relevante frente la " *pérdida de confidencialidad e integridad de la información, debido a las malas prácticas del uso de la cuenta de correo*"; esto se refiere considerando que el control descrito debe ajustarse indicando cual es la acción/verbo rector que indique control (*Verificar, validad, hacer seguimiento, etc*) y porque debería existir un control a cargo del proceso / dependencia responsable del activo, que indique la(s) acción(es) frente al riesgo identificado, especialmente en cuanto al tema de uso de la cuenta e información que allí se recibe o manejo que se da que debe ser confidencial o de reserva para generar confianza al denunciante). Por otra parte, en las evidencias de ejecución del control se refieren capacitaciones, lo cual debería disponerse en el plan de manejo y no en la actividad de control además porque no se describen dentro del mismo. En cuanto al Plan de Manejo de Riesgos, se presentan las mismas de la actividad de control y no se aportan resultados del monitoreo *mensual,* la acción se describe como actividad de control, por lo cual se sugiere replantear tanto acción del Plan de Manejo así como la actividad de control y definir adecuadamente las evidencias de cada una.
4	Posibilidad de afectación reputacional debido al acceso no autorizado de personal sin vinculo contractual vigente y/o de sus terceros con la ART, por la no protección de la información privada referente a las huellas dactilares.	La solicitud de acceso inicia con un correo institucional emitido por el jefe o coordinador del área, en el cual se indica el nombre del funcionario y/o contratista que requiere el ingreso. El profesional encargado del área administrativa recibe la solicitud y valida la vigencia de la solicitud, la pertinencia del acceso y la autorización correspondiente. Una vez verificada la información, se configuran los permisos en el sistema biométrico, garantizando que solo el personal activo y autorizado pueda ingresar a las áreas restringidas. Se mantiene una lista actualizada de personal con acceso autorizado, la cual es validada mensualmente por los GIT de Talento Humano y Administrativa. Como respaldo del proceso, se conservan los formatos de control de acceso firmados durante el periodo correspondiente, asegurando la trazabilidad y evidencia del control.	Se verifica mensualmente que no tengan acceso funcionarios y/o contratistas a las instalaciones cuando ya se han desvinculado de la entidad	Indeterminado	Se observan debilidades en el diseño del control debido a que no se describen las desviaciones y acciones en caso de presentarse; respecto a las evidencias, se presentan algunos soportes de solicitudes de acceso y soportes de pazysalvos, sin embargo no se cuenta con soporte de ejecución de la actividad de control referida, es decir de la validación, verificación y de la lista actualizada de personal con acceso autorizado, *la cual es validada mensualmente.* Respecto al Plan de Manejo, no se aportan evidencias de la verificación mensual como se menciona en la acción, se presentan las mismas evidencias de la actividad de control por lo cual no es posible validar si se encuentra en ejecución.

N	RIESGO	Controles	Acciones Plan de Manejo	Estado Acciones Plan de Manejo	Observaciones frente al diseño y ejecución del Control y acciones del Plan de Manejo (Según Evidencias)
5	Posibilidad de afectación reputacional por acceso no autorizado, generando pérdida de integridad y confidencialidad de la información, debido a cambios de usuarios y roles en los procesos	Cada vez que se realice una solicitud de acceso por cada dependencia, el responsable de la mesa de servicio, verifica: El diligenciamiento de formato de control de acceso(FM-TI-07.V7 Formato de control de accesos). Con el fin de Remitirlo al área de SI para su aprobación y proceder a conceder los permisos a los usuarios. En este particular la secion correspondiente al SGO. En caso de encontrar que el formato no se encuentre debidamente diligenciado se devuelve al peticionario a través del caso de la mesa de servicio. Evidencias formatos de control de acceso firmados mes a mes durante el periodo.	Se verifica trimestralmente la realización de la depuración de usuarios que en la aplicación han tenido gestión de creación, inactivación o reactivación de usuarios y modificación de roles	En Ejecución con debilidades en evidencias	Se observa con la descripción del control que se cumplen los criterios. Se encuentran en las evidencias: Listado de usuarios activos al corte de septiembre y Archivo de solicitudes al corte de junio de 2025, las cuales se sugiere incluir en la actividad de control como evidencias de ejecución teniendo en cuenta que las mismas soportan la actividad más que los formatos de solicitud de acceso y pazysalvos. Respecto al Plan de Manejo de riesgos, se refieren los mismos que en la actividad de control por lo cual se sugiere conservar únicamente los registros de la verificación trimestral y para la actividad de control considerando que es a demanda, verificar y/o contar con los soportes de cada solicitud.
6	Posibilidad de afectación reputacional por acceso no autorizado, generando pérdida de integridad de la información, debido al acceso no autorizado de personal por cambio de área	Cada vez que se realice una solicitud de acceso por cada dependencia al sistema de gestión documental Orfeo, el jefe solicitante envía correo de solicitud de creación de usuario en el sistema mencionado al GIT de administrativa al profesional encargado, este usuario asignado se relaciona con el directorio activo de la entidad. Se ajusta a los roles solicitados y permisos correspondientes.	Se verifica trimestralmente la realización de la depuración de usuarios que en la aplicación han tenido gestión de creación, inactivación o reactivación de usuarios y modificación de roles	En Ejecución con debilidades en evidencias	La actividad descrita como tal no es un control sino una actividad de gestión, no cumple con los requisitos de: definir verbo de control y con base en ello describir lo que se verifica, valida, revisa, hace seguimiento, etc; no se describen desviaciones y acciones generadas de las mismas. Se aporta como evidencia ejemplos de formatos de control de accesos, sin embargo, se deben verificar las solicitudes y gestiones realizadas desde la 2a línea de defensa (OTI). Se requiere ajustar para que sea un control. Respecto al Plan de Manejo de Riesgos, se aportan: archivo de "Reporte de novedades Usuarios ORFEO" y "Usuarios Activos/inactivos ORFEO", no obstante, no es posible determinar a qué periodo o corte corresponden; se sugiere contar con las evidencias de manera trimestral tal como se determina en la acción del plan.
7	Posibilidad de afectación económica y reputacional por acceso no autorizado, generando perdida de integridad de la información, ocasionando una mala gestión administrativa del ERP.	Cada vez que se realice una solicitud de acceso por cada dependencia, el responsable de la mesa de servicio, verifica: El Diligenciamiento de formato de control de acceso(FM-TI-07.V7 Formato de control de accesos). Con el fin de Remitirlo al área de SI para su aprobación y proceder a conceder los permisos a los usuarios. En caso de encontrar que el formato no se encuentre debidamente diligenciado se devuelve al peticionario a través del caso de la mesa de servicio. Evidencias formatos de control de acceso firmados mes a mes durante el periodo.	Mensualmente se realiza la revisión, ajuste o inactivación de los roles asignados a los colaboradores que han tenido gestión de altas, bajas o modificaciones en sus funciones.	Indeterminado	Se observa con la descripción del control que se cumplen los criterios, sin embargo, es pertinente incluir como soporte del control, los correos enviados en caso de encontrar desviaciones de acuerdo a lo descrito. No porque no se tengan sino porque no se aportaron en la carpeta de evidencias y no se refieren en la columna de evidencias. Respecto al Plan de Manejo de Riesgos, se debe contar con una evidencia que permita identificar los resultados del seguimiento realizado mensualmente como se describe (si es el caso sobre una muestra verificada, con fechas, entre otros) que registre los resultados de si efectivamente los funcionarios/contratistas desvinculados a la ART no tienen acceso a SYNERSIS

N	RIESGO	Controles	Acciones Plan de Manejo	Estado de Acciones Plan de Manejo	Observaciones frente al diseño y ejecución del Control y acciones del Plan de Manejo (Según Evidencias)
8	Posibilidad de afectación reputacional por cualquier posible de ataque informático, generando perdida de seguridad de la información, ocasionando una mala reputacion a nivel nacional al tener el sitio web inoperativo.	El SOC con una periodicidad mensual ejecuta pruebas de seguridad la infraestructura tecnológica incluida la página web de la entidad, se realizan escaneos automatizados utilizando herramientas autorizadas, El responsable de infraestructura revisa los reportes generados. Los hallazgos se remiten formalmente al profesional encargado de comunicaciones para la aplicación de los parches o correcciones. Una vez corregidas las vulnerabilidades, se ejecuta una nueva revisión técnica para validar la efectividad de las acciones	Mensualmente se realiza la verificación técnica de la página web institucional mediante mecanismos automatizados de escaneo de vulnerabilidades proporcionados por el Centro de Operaciones de Seguridad (SOC). El SOC ejecuta las pruebas desde herramientas especializadas que permiten identificar configuraciones inseguras, versiones obsoletas de componentes o posibles vectores de ataque.	Indeterminado	Se observa con la descripción del control que se cumplen los criterios, sin embargo es pertinente contar con las evidencias de ejecución mes por mes en el repositorio toda vez que solo se aportó como evidencia el ultimo realizado, o dar constancia de lo revisado por la 2a línea de defensa en caso de no ser posible su recopilación. Respecto al Plan de Manejo de Riesgos, se determinó la misma actividad de control y evidencias por lo cual se sugiere analizar si existen actividades adicionales que complementen la actividad de control.
9	Posibilidad de afectación reputacional por cualquier posible de ataque informático, generando perdida de seguridad de la información, ocasionando una mala reputación a nivel nacional al perder cualquier canal oficial de la ART	Trimestralmente, en coordinación con los profesionales encargados del área de Comunicaciones de la ART, se valida que los canales oficiales de comunicación e interacción digital incluidos aplicativos, redes sociales, sitio web institucional, mantengan medidas activas de protección contra suplantación y accesos no autorizados. La verificación incluye la comprobación de autenticación multifactor (MFA) en las cuentas administradoras, la revisión de configuraciones de seguridad y roles de acceso, y la confirmación de la oficialidad de los dominios, perfiles y plataformas asociadas a la entidad.	Implementar mecanismos trimestralmente automatizados para mantener un registro consolidado del estado de MFA en todas las redes institucionales, asegurando la corrección inmediata ante cualquier desviación detectada.	En Ejecución con debilidades en evidencias	Se observa con la descripción del control que se cumplen parcialmente los criterios pero no se describen las desviaciones y acciones que se generan con su respectiva evidencia. En las evidencias aportadas (del seguimiento realizado por la 2a Línea de defensa), se encuentran soportes de Implementación de factor de doble autenticación e Implementación de políticas de gestión de contraseñas seguras y uso de herramientas de gestión de contraseñas, sin embargo de acuerdo a lo descrito en el control, se deberían tener los reportes trimestrales o soporte de verificación trimestral de la validación que realizan los responsables (ej, acta, informe, reporte) puesto que las evidencias relacionadas no son consistentes o no evidencian como se realiza la validación y resultados, adicionalmente que podrían generar como producto de desviaciones. Se incluye como evidencia el manual de políticas de SI lo cual también es inconsistente. Respecto al Plan de Manejo, se aportan evidencias de la actividad de control, se observa un reporte con listado de funcionarios con cuentas MFA activo que no registra fecha. Se sugiere contar con evidencias consistentes a lo descrito tanto para la actividad de control como para la acción del plan de manejo de riesgos.

N	RIESGO	Controles	Acciones Plan de Manejo	Estado de Acciones Plan de Manejo	Observaciones frente al diseño y ejecución del Control y acciones del Plan de Manejo (Según Evidencias)
10	Posibilidad de afectación económica y reputacional por exposición de información confidencial o pérdida de su integridad debido a accesos no autorizados o filtración de datos, generada por vulnerabilidades en los protocolos de acceso a las bases de datos	El SOC con una periodicidad mensual ejecuta pruebas de seguridad la infraestructura tecnológica, se realizan escaneos automatizados utilizando herramientas autorizadas, El responsable de infraestructura revisa los reportes generados. Los hallazgos se remiten formalmente al profesional encargado como DBA para la aplicación de los parches o correcciones. Una vez corregidas las vulnerabilidades, se ejecuta una nueva revisión técnica para validar la efectividad de las acciones	Mensualmente se realiza la verificación técnica de las bases de datos institucionales mediante mecanismos automatizados de escaneo de vulnerabilidades proporcionados por el Centro de Operaciones de Seguridad (SOC). El SOC ejecuta las pruebas utilizando herramientas especializadas que permiten identificar configuraciones débiles, versiones obsoletas de motores de base de datos, parches pendientes o exposiciones en servicios de conexión. Los resultados del escaneo son analizados por el líder de infraestructura, quien prioriza los hallazgos según su criticidad y coordina la aplicación de las medidas correctivas si en el mismo se reportan eventos con las bases de datos. Los informes generados se documentan como evidencia del control y seguimiento mensual.	En Ejecución con debilidades en evidencias	Se observa con la descripción del control que se cumplen los criterios. Se tienen informes mensuales de "ANÁLISIS DE REGISTROS DE TRANSACCIÓN Y CONFIGURACIÓN DE BASE DE DATOS." y soporte de informes y correos del seguimiento del mes de septiembre, (pendiente consolidar los soportes de todos los meses en el repositorio de seguimiento al Mapa de Riesgos) Respecto al Plan de Manejo de Riesgos, se determinó la misma actividad de control y evidencias solo que descrita más a detalle, por lo cual se sugiere analizar si existen actividades adicionales que complementen la actividad de control o si la acción del plan de manejo se ajusta más a una actividad de control.
11	Posibilidad de afectación económica y reputacional por pérdida de la integridad y disponibilidad de los datos debido a vulnerabilidades explotables en el motor de base de datos, generado por el uso de versiones desactualizadas	El SOC con una periodicidad mensual ejecuta pruebas de seguridad la infraestructura tecnológica de la entidad, se realizan escaneos automatizados utilizando herramientas autorizadas, El responsable de infraestructura revisa los reportes generados. Los hallazgos se remiten formalmente al profesional encargado como DBA para la aplicación de los parches o correcciones al motor de bases de datos. Una vez corregidas las vulnerabilidades, se ejecuta una nueva revisión técnica para validar la efectividad de las acciones	"Mensualmente se realiza la verificación técnica de las bases de datos institucionales mediante mecanismos automatizados de escaneo de vulnerabilidades gestionados por el Centro de Operaciones de Seguridad (SOC). El SOC ejecuta las pruebas sobre los entornos de producción y pruebas, utilizando herramientas especializadas que permiten identificar versiones obsoletas del motor de base de datos, configuraciones inseguras, servicios expuestos, credenciales débiles, parches pendientes o permisos excesivos en los usuarios. Los resultados del escaneo son analizados por el líder de infraestructura, quien prioriza los hallazgos según su criticidad y coordina la aplicación de las medidas correctivas si en el mismo se reportan eventos con los motores de bases de datos. Los informes generados se documentan como evidencia del control y seguimiento mensual."	En Ejecución con debilidades en evidencias	Se observa con la descripción del control que se cumplen los criterios. Se observa reporte del SOC y soporte de informe de vulnerabilidades, correos y cierre de hallazgos del seguimiento del mes de septiembre, (pendiente consolidar los soportes de todos los meses en el repositorio de seguimiento al Mapa de Riesgos) Respecto al Plan de Manejo de Riesgos, se determinó la misma actividad de control y evidencias solo que descrita más a detalle, por lo cual se sugiere analizar si existen actividades adicionales que complementen la actividad de control o si la acción del plan de manejo se ajusta más a una actividad de control.

N	RIESGO	Controles	Acciones Plan de Manejo	Estado de Acciones Plan de Manejo	Observaciones frente al diseño y ejecución del Control y acciones del Plan de Manejo (Según Evidencias)
12	Posibilidad de impacto económico, reputacional o de operación debido al uso de herramientas de despliegue y desarrollo obsoletas, errores de desarrollo, debilidades en el código fuente por prácticas de desarrollo inseguras, falta de revisiones de código o por la inclusión de dependencias o bibliotecas externas no seguras, las cuales podrían comprometer la confidencialidad, integridad o disponibilidad de los datos, sistemas y servicios de la Entidad.	El SOC con una periodicidad mensual ejecuta pruebas de seguridad la infraestructura tecnológica de la entidad, se realizan escaneos automatizados utilizando herramientas autorizadas, El responsable de infraestructura revisa los reportes generados. Los hallazgos se remiten formalmente al profesional encargado para la aplicación de los parches o correcciones. Una vez corregidas las vulnerabilidades, se ejecuta una nueva revisión técnica para validar la efectividad de las acciones	Mensualmente se realiza la verificación técnica de seguridad sobre las aplicaciones en desarrollo mediante escaneos automatizados de vulnerabilidades gestionados por el Centro de Operaciones de Seguridad (SOC). El SOC ejecuta los análisis utilizando herramientas especializadas que permiten detectar fallos de seguridad en el código fuente, dependencias obsoletas, configuraciones inseguras en entornos de prueba, exposición de credenciales y componentes vulnerables. Los resultados del escaneo son analizados por el líder de infraestructura, quien prioriza los hallazgos según su criticidad y coordina la aplicación de correcciones, parches o refactorización de código. Cada revisión se documenta en un informe técnico y se valida que los hallazgos críticos sean corregidos antes de avanzar hacia el entorno productivo	En Ejecución con debilidades en evidencias	Se observa con la descripción del control que se cumplen los criterios. Se observa reporte del SOC y soporte de informe de vulnerabilidades, correos y cierre de hallazgos del seguimiento del mes de septiembre, (pendiente consolidar los soportes de todos los meses en el repositorio de seguimiento al Mapa de Riesgos) Respecto al Plan de Manejo de Riesgos, se determinó la misma actividad de control y evidencias solo que descrita más a detalle, por lo cual se sugiere analizar si existen actividades adicionales que complementen la actividad de control o si la acción del plan de manejo se ajusta más a una actividad de control.
13	Posibilidad de afectación económica y reputacional por pérdida de la integridad y disponibilidad de activos de información debido a vulnerabilidades explotables en el sistema operativo, generado por el uso de versiones desactualizadas	El SOC con una periodicidad mensual ejecuta pruebas de seguridad la infraestructura tecnológica de la entidad, se realizan escaneos automatizados utilizando herramientas autorizadas, El responsable de infraestructura revisa los reportes generados. Los hallazgos se remiten formalmente al profesional encargado de la administración de los servidores, para la aplicación de los parches o correcciones. Una vez corregidas las vulnerabilidades, se ejecuta una nueva revisión técnica para validar la efectividad de las acciones	Mensualmente se realiza la verificación técnica de seguridad sobre los servidores físicos y virtuales mediante mecanismos automatizados de escaneo de vulnerabilidades gestionados por el Centro de Operaciones de Seguridad (SOC). El SOC ejecuta los escaneos utilizando herramientas especializadas que permiten identificar sistemas operativos desactualizados, configuraciones inseguras, servicios expuestos, parches pendientes, cuentas privilegiadas no controladas y vulnerabilidades en servicios críticos. Los resultados de los análisis son revisados por el líder de infraestructura, quien evalúa los hallazgos, determina su criticidad y coordina la aplicación de las acciones correctivas o actualizaciones necesarias. Cada revisión se documenta en un reporte técnico, y los hallazgos críticos son priorizados para su atención inmediata.	En Ejecución con debilidades en evidencias	Se observa con la descripción del control que se cumplen los criterios. Se observa reporte del SOC y soporte de informe de vulnerabilidades, correos y cierre de hallazgos del seguimiento del mes de septiembre, (pendiente consolidar los soportes de todos los meses en el repositorio de seguimiento al Mapa de Riesgos) Respecto al Plan de Manejo de Riesgos, se determinó la misma actividad de control y evidencias solo que descrita más a detalle, por lo cual se sugiere analizar si existen actividades adicionales que complementen la actividad de control o si la acción del plan de manejo se ajusta más a una actividad de control.

N	RIESGO	Controles	Acciones Plan de Manejo	Estado de Acciones Plan de Manejo	Observaciones frente al diseño y ejecución del Control y acciones del Plan de Manejo (Según Evidencias)
14	Posibilidad de afectación económica por pérdida de disponibilidad del centro de datos debido al ingreso no autorizado de personas ajenas a la operación, o por riesgo de inundación o incendio que podrían generar daños irreparables a equipos o la interrupción prolongada de las operaciones	Revisar el mecanismo de ingreso al centro de datos, que los profesionales que ingresan al Datacenter son los autorizados por el jefe de la OTI que pertenecen a esa dependencia y tienen relación directa con la infraestructura tecnológica en sus obligaciones y/o funciones. Que ninguna persona permanezca sola en el centro de datos, salvo autorización especial. En un registro de bitácora se registra; nombre del visitante, hora de ingreso y salida, actividad realizada.	El acceso a los centros de cableado se encuentra restringido al personal autorizado, validado mediante el sistema biométrico institucional. Personal ajeno a la oficina de Tecnologías se registra en la bitácora de acceso, donde se consignan la fecha, hora, motivo y persona responsable del acompañamiento. Durante la visita, el ingreso se realiza en compañía de un custodio o funcionario designado que supervisa las actividades ejecutadas dentro del área restringida, garantizando que no se manipulen equipos, cableado o dispositivos sin la debida autorización.	Indeterminado	Se observan debilidades en redacción toda vez que no se determina el responsable de la ejecución del control, no se determina periodicidad de ejecución y el propósito no deriva ni describe desviaciones y en que se soportan tanto la actividad de control como las desviaciones; de acuerdo a lo descrito, se presentan las bitácoras de ingreso al Datacenter pero no se describe la evidencia producto de la revisión que se hace cual seria, adicionalmente porque se aporta el Manual de Políticas de Seguridad de la información pero no es una evidencia generada de la actividad de control. Se debe ajustar el control de acuerdo a la metodología con el fin de que se evidencie lo que realmente se realiza, verifica o revisa. Respecto al Plan de Manejo de riesgos, la acción descrita no determina puntualmente la "acción" complementaria a realizar para fortalecer los controles o atacar las causas
15	Posibilidad de afectación económica por pérdida de disponibilidad del centro de datos debido a la falta de aislamiento de los equipos propios del centro de datos, o por riesgo de inundación o incendio que podrían generar daños irreparables a equipos o la interrupción prolongada de las operaciones	El ingeniero designado por el jefe de la OTI verifica semestralmente a través de una lista de chequeo la conformidad de los elementos que componen el sistema de detección de incendios. En caso de encontrar inconformidades, reporta al jefe de la OTI para tomar decisiones frente al restablecimiento del tema tratado.	Realizar dos inspecciones técnicas en el centro de datos para verificar el aislamiento físico y ambiental de los equipos críticos, asegurando que los racks y servidores estén separados de materiales combustibles o fuentes de calor.	En ejecución	La actividad descrita no corresponde a una actividad de control y presenta debilidades en su redacción debido a que no tiene responsables, no se describe en que consiste la verificación sobre un medio o herramienta de control aplicable, cuando o como, no menciona periodicidad, y no se describen las desviaciones y evidencias que se puedan generar, así como las acciones a seguir. Las evidencias aportadas además no son consistentes (capacitación brigada de incendios, inventario de extintores, Manual de Políticas de SI y Plan de Emergencias). Respecto al Plan de Manejo de Riesgos, no se presentan soportes de las inspecciones trimestrales realizadas, se aportan capacitaciones e inventario lo cual no es consistente con lo descrito en la acción.
16	Posibilidad de afectación económica por hurto o pérdida de computadores portátiles y/o dispositivos de almacenamiento externo con información confidencial de la Entidad. Infección de malware por uso de dispositivos externos de almacenamiento de dudosa procedencia o manipulación	Anualmente la ART contrata una póliza de seguros que incluye el aseguramiento de los equipos de cómputo. En caso de hurto o pérdida de los equipos de cómputo estos se repondrán a través del uso de dicha póliza. Cuando exista pérdida de información por hurto, pérdida e, se reestablece a través de los repositorios en nube que se destinan a cada equipo. Adicionalmente se verifica por el delegado de la OTI que los equipos cuenten con protección antivirus para protección de malware."	Realizar sensibilizaciones frente a hurto a los funcionarios y contratistas	Pendiente de ejecución	Se observa que el riesgo tiene dos componentes que ameritan dividirlo, se redactó con dos posibles amenazas por lo cual es necesario ajustar y separar identificando actividades de control por separado. Se observa con la descripción del control que se cumplen los criterios sin embargo al ser un control correctivo las verificaciones se aplican de manera aleatoria (cuando se materializa y se aplica la desviación). Adicionalmente se observa que el control se define como preventivo y corresponde a un control correctivo. Respecto al Plan de Manejo de Riesgos, se han hecho capacitaciones en S.I., sin embargo, se encuentra por ejecutar la sensibilización programada en el Plan.

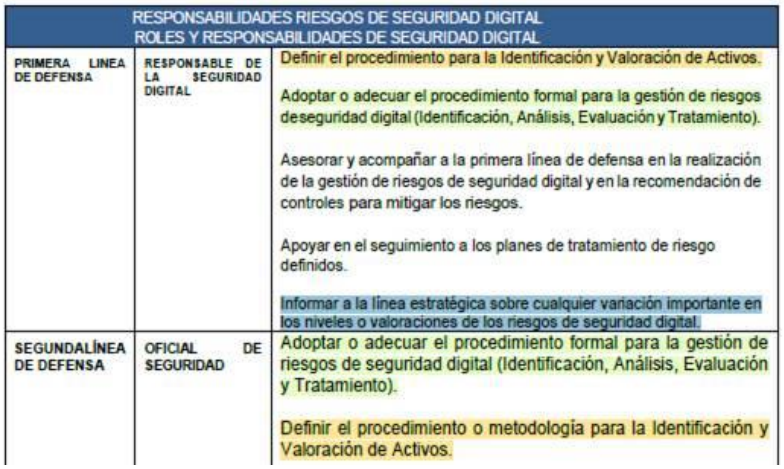
N	RIESGO	Controles	Acciones Plan de Manejo	Estado Acciones Plan de Manejo	Observaciones frente al diseño y ejecución del Control y acciones del Plan de Manejo (Según Evidencias)
17	Posibilidad de afectación económica por accesos no autorizados y filtración de datos, pérdidas de disponibilidad por fallas de seguridad o ataques y propagación de malware en archivos compartidos en servicios en nube.	El administrador de la red en nube verifica que los proveedores de servicios cuentan con mecanismos de autenticación multifactor (2FA/MFA) a través de reportes del MFA, además la aplicación de políticas de contraseñas, la integración con el directorio corporativo, y la revisión de los niveles de servicio y seguridad definidos contractualmente, con el fin de mantener y asegurar la protección de los activos tecnológicos bajo responsabilidad de la OTI. En caso de encontrar vulneraciones a las políticas de contraseñas por acceso no autorizado se gestionará un incidente de seguridad por la MDS para realizar las correcciones necesarias	Se realiza la coordinación técnica y administrativa con los proveedores de servicios por parte del líder de infraestructura mediante reuniones programadas o revisiones trimestrales de cumplimiento, donde se validan las configuraciones y controles de autenticación implementados.	Indeterminado	Se observa con la descripción del control que se cumplen los criterios. En las evidencias de ejecución, se tienen documentos contractuales de órdenes de compra " ADQUISICION DE SERVICIOS DE MICROSOFT AZURE PARA RENOVAR EL SISTEMA DE NUBE ACTUAL PARA LA DIRECCION DE INFORMACION Y PROSPECTIVA", ACUERDO DE NIVEL DE SERVICIO, Reporte de Cuentas MFA usuarios activos y soporte de seguimiento (archivo word) *EVIDENCIA PLAN DE ACCIÓN RIESGOS SEGURIDAD DE LA INFORMACIÓN* con pantallazos de la aplicación y ejecución del control. Respecto al Plan de Manejo de Riesgos, se presentan los mismos soportes de la "actividad de control", se encuentran pendientes de consolidar los soportes de las reuniones trimestrales realizadas en el repositorio donde se validan las configuraciones y controles de autenticación implementados.
18	Posibilidad de afectación económica y de operación por fallas en la configuración o en la operatividad de los sistemas o riesgo de desactualización por falta de recursos para su gestión y actualización	El SOC con una periodicidad mensual ejecuta pruebas de seguridad la infraestructura tecnológica, se realizan escaneos automatizados utilizando herramientas autorizadas, El responsable de infraestructura revisa los reportes generados. Los hallazgos se remiten formalmente al profesional encargado de la mesa de ayuda para la aplicación de los parches o correcciones. Una vez corregidas las vulnerabilidades, se ejecuta una nueva revisión técnica para validar la efectividad de las acciones	Mensualmente se realiza la verificación técnica de protección antimalware y respaldo de información sobre los equipos y servidores institucionales. El Centro de Operaciones de Seguridad (SOC) supervisa el estado y actualización del antivirus corporativo, validando que las firmas de detección, motores de análisis y configuraciones de protección en tiempo real se encuentren activos y actualizados. Paralelamente, se realizan copias de respaldo por parte del profesional encargado de la OTI para confirmar la ejecución exitosa de las rutinas automáticas, la integridad de los archivos respaldados y la disponibilidad de medios de recuperación.	En Ejecución con debilidades en evidencias	Se observa con la descripción del control que se cumplen los criterios. Respecto al Plan de Manejo de Riesgos, se presenta como evidencia pruebas de antivirus, SIEM, ARCSERVE; sin embargo es pertinente dejar el registro mensual con los resultados de la verificaciones realizadas donde se explique claramente las pruebas ejecutadas y resultados así como detección de desviaciones y acciones implementadas, y no solamente pantallazos. Esto con el fin de dar claridad a lo que se ejecuta.

Fuente: Papel de trabajo evaluación riesgos SI

8. OPORTUNIDADES DE MEJORAMIENTO

A continuación, se relacionan los HALLAZGOS identificados con la letra "H" y las OBSERVACIONES identificadas con la letra "O"

N°	TIPO	DESCRIPCIÓN
1	O	Se observan debilidades en el diseño, ejecución y/o registros de los controles correspondientes a los Riesgos 3, 4, 6, 9 y 14, de los cuales, 3 controles se encuentran en nivel Regular calificados con 60 puntos y dos en nivel Adecuado calificados con 80 puntos, sobre los cuales se presentan las observaciones al detalle en el numeral 7.2 – tabla 4 con el fin de subsanar y establecer las acciones de mejora pertinentes, que no de no ajustarse y contar con las evidencias, podrían impactar en el Sistema de Gestión de Seguridad de la Información por no contar con controles que sean efectivos para el logro de los objetivos y que permitan detectar y tratar inconsistencias (desviaciones) adecuadamente.
2	O	En el Manual de Política de Riesgos de la ART, versión 2025, páginas 33 y 36, se describen los roles y responsabilidades de Seguridad Digital, se observan dos actividades a cargo de dos responsables que son exactamente iguales; Adicionalmente, se define como primera línea de defensa al "RESPONSABLE DE LA SEGURIDAD DIGITAL", pero se asignan funciones o actividades de Segunda Línea de Defensa así*: "Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital…Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad digital y en la recomendación de controles para mitigar los riesgos"* (como se vislumbra a continuación).



RESPONSABILIDADES RIESGOS DE SEGURIDAD DIGITAL ROLES Y RESPONSABILIDADES DE SEGURIDAD DIGITAL		
PRIMERA LINEA DE DEFENSA	RESPONSABLE DE LA SEGURIDAD DIGITAL	Definir el procedimiento para la Identificación y Valoración de Activos. Adoptar o adecuar el procedimiento formal para la gestión de riesgos deseguridad digital (Identificación, Análisis, Evaluación y Tratamiento). Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad digital y en la recomendación de controles para mitigar los riesgos. Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos. Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital.
SEGUNDALÍNEA DE DEFENSA	OFICIAL DE SEGURIDAD	Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, Análisis, Evaluación y Tratamiento). Definir el procedimiento o metodología para la Identificación y Valoración de Activos.

Lo anterior genera confusión en cuanto a las responsabilidades a cargo de cada Rol y hace necesario definir considerando que hacen parte de la primera línea de defensa los lideres de procesos a cargo de activos de información con sus respectivos riesgos y controles asociados, con el apoyo de la OTI como segunda línea de defensa.

9. RECOMENDACIONES

Se recomienda a los responsables de primera línea de defensa revisar las observaciones descritas en los informes presentados por el GIT de Control Interno con el fin de aplicar los correctivos necesarios a las características del diseño y ejecución o documentación de los controles que presentan debilidades con el fin de optimizarlos y que los mismos apunten a evitar la materialización de riesgos identificados

en cada uno de los procesos, esto puede realizarse mediante mesas de trabajo entre la primera y segunda línea de defensa, en donde se realice un proceso de actualización de acuerdo con los lineamientos establecidos en el Manual de Riesgos de la ART y Modelo de Seguridad y Privacidad de la Información emitido por el MinTic, versión 5 del 21/04/2025.

Se sugiere ajustar el Manual de Política de Administración del Riesgo POL-DE-08 V1 en lo que se refiere a los riesgos de seguridad digital, en el tema de Roles y responsabilidades y adaptándose a los cambios referidos en la última versión del MSPI emitida por el Ministerio de TIC en 2025.

10. CONCLUSIONES

Se evaluó el diseño y ejecución de los controles de Seguridad digital, así como su pertinencia de acuerdo a los riesgos identificados en la Matriz de Riesgos de Seguridad de la Información encontrando conformidad de los controles con un nivel promedio de evaluado como SATISFACTORIO.

Se verificó el diseño y ejecución de los controles a partir de los criterios definidos en la metodología y a partir de ello determinar si son adecuados para evitar la materialización de riesgos con lo cual se concluye que de 18 controles determinados en la matriz de riesgos de Seguridad de la Información, 13 controles se encuentran en nivel “Optimo” respecto a su diseño y ejecución calificados en promedio con 98 puntos, 2 controles valorados en un nivel “Adecuado” con 80 puntos y sobre los cuales se deben generar mejoras en su diseño, 3 en nivel “Regular” que ameritan correcciones y ajustes en cuanto a diseño y ejecución especialmente en la definición de responsables y evidencias, y 3 en un Nivel “Deficiente” debido a que como están descritos no corresponden a las características de diseño de controles efectivos.

Se verificó que se está realizando el seguimiento a la ejecución de los controles y acciones del plan de manejo de riesgos por parte de la OTI como segunda línea de defensa sin embargo se debe mejorar la organización del repositorio de evidencias considerando que no fue posible determinar en porcentaje de avance el estado de las actividades de acuerdo a los soportes presentados.

11. FIRMAS RESPONSABLES

Auditor: 	**Vo. Bo** MARLON SALOMON CONTRERAS TURBAY Firmado digitalmente por MARLON SALOMON CONTRERAS TURBAY Fecha: 2025.11.04 17:16:19 -05'00'
NOMBRE: MARISOL GUTIERREZ HERNANDEZ **CARGO: CONTRATISTA GITCI**	**NOMBRE: MARLON SALOMON CONTRERAS TURBAY** **CARGO: Coordinador GIT de Control Interno**
FECHA DE INFORME:	**31 de Octubre de 2025**