ALCALDÍA MAYOR DE BOGOTÁ
SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA
AL RESPONDER CITAR EL NR.
Nro. Rad: 3-2025-7706
Fecha: 26/02/2025 12:16:06 PM
Destino: 100-DESPACHO

MEMORANDO

Para: CESAR ANDRES RESTREPO FLOREZ
DESPACHO SECRETARIO DE SEGURIDAD

De: OFICINA DE CONTROL INTERNO

Asunto: INFORME DE SEGUIMIENTO A CONTROLES ASOCIADOS A RIESGOS DE SEGURIDAD DE LA INFORMACION CORRESPONDIENTE AL TERCER CUATRIMESTRE DE 2024

Cordial saludo, Dr. Restrepo Florez:

Respecto a lo estipulado Artículo 17 del Decreto 648 de 2017 respecto del rol ”Evaluación de la Gestión del Riesgo” emitido por el Departamento Administrativo de la Función Pública, así como en el cumplimiento de la ejecución del Plan Anual de Auditoría vigencia 2025 y la Política de Administración de Riesgos de la Secretaría Distrital de Seguridad, Convivencia y Justicia (PO-FI-02 V2); la Oficina de Control Interno se permite comunicar el **Informe de seguimiento a controles asociados a los Riesgos de Seguridad de la Información,** correspondiente al tercer cuatrimestre de 2024, con los resultados obtenidos.

A partir de los resultados se sugiere tener en cuenta las recomendaciones indicadas en el presente informe con el fin de identificar acciones que permitan coadyuvar con el mejoramiento continuo y fortalecimiento institucional, principalmente en materia de seguridad digital y de la información.

Finalmente, es preciso informar que, el informe adjunto será publicado en la sección de transparencia de la entidad en la siguiente ruta[1]: Botón Transparencia y Acceso a la Información Pública → Planeación, Presupuesto e Informes → Informe de la Oficina de Control Interno → Informes de Ley y/o Seguimiento→ 2025.

Cordialmente,

[1] https://scj.gov.co/es/transparencia/planeacion-presupuesto-ingresos/informes-control-interno

Av. Calle 26 # 57- 83
Torre 7 Tel: 3779595
Código Postal: 111321
www.scj.gov.co

ALCALDÍA MAYOR DE BOGOTÁ
SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA
AL RESPONDER CITAR EL NR.
Nro. Rad: 3-2025-7706
Fecha: 26/02/2025 12:16:06 PM
Destino: 100-DESPACHO

KAROL ANDREA PARRAGA HACHE
JEFE DE OFICINA CONTROL INTERNO

c.c.e.: IVAN HERSAYN PINILLA HERRERA-DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION
ARIEL HERNAN LAYTON COY-OFICINA ASESORA DE PLANEACION
Anexos: -1

Elaboró: DIEGO ALEXANDER URAZAN FRANCO
Revisó: DIEGO ALEXANDER URAZAN FRANCO-OFICINA DE CONTROL INTERNO -
Aprobó: KAROL ANDREA PARRAGA HACHE

Av. Calle 26 # 57- 83
Torre 7 Tel: 3779595
Código Postal: 111321
www.scj.gov.co

Informe de seguimiento a riesgos de seguridad de seguridad de la información - tercer cuatrimestre de 2024

2025

Oficina de Control Interno

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA
BOGOTÁ

1. OBJETIVO

Evaluar y realizar seguimiento a la implementación, diseño y gestión de los controles a través de los cuales se administran los Riesgos de Seguridad de la información en la Secretaría Distrital de Seguridad, Convivencia y Justicia, de acuerdo con la PO-FI-02 Política de administración de Riesgos V2 y la G-FI-04 Guía de Administración de Riesgos. V3, que forman parte del Sistema Integrado de Gestión - SIG.

1.1. Objetivos específicos:

- Validar si los Riesgos de Seguridad de la información identificados por los procesos cumplen con lo establecido en la Política de Administración de Riesgos de la Entidad PO-FI-02- V2.
- Verificar si los procesos de la SDSCJ cuentan con controles asociados a Seguridad de la información.
- Revisar la estructura, diseño y ejecución de los controles asociados a los Riesgos de Seguridad de la información vigentes.
- Efectuar seguimiento de la gestión realizada con base en las recomendaciones emitidas por la Oficina de Control Interno a través de los informes periódicos de la vigencia 2024.

2. ALCANCE

El ejercicio de evaluación y seguimiento comprende el periodo entre el 01 de septiembre y el 31 de diciembre de 2024, en referencia a la Matriz de Riesgos de Seguridad de la Información (F-FI-1385) vigente y a las evidencias aportadas por los procesos.

Lo anterior, teniendo en cuenta que, el numeral 13. Titulado PUBLICACIÓN, SEGUIMIENTO Y EVALUACIÓN A LOS RIESGOS de la citada Política de administración de riesgos PO-FI-02 V2, la cual establece que, corresponde a la Primera Línea de Defensa realizar el cargue de soportes documentales de la implementación de los controles; y a la Segunda Línea de Defensa realizar cuatrimestralmente el seguimiento a la Matriz de Riesgos y remitir informe del resultado a la Oficina de Control Interno.

3. CRITERIOS DE AUDITORÍA

- Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6, emitida por el DAFP.
- Guía de Administración del Riesgo de la SDSCJ (G-FI-04 V3).
- Política de Administración de Riesgos de la SDSCJ (PO-FI-02 V2).
- Política de Seguridad y Privacidad Información de la SDSCJ (PO-GT-1).
- Matriz de Riesgos de Seguridad de la Información de la Entidad (F-FI-1385).

4. SEGUIMIENTO DE AUDITORÍA

4.1. Cumplimiento Política administración de riesgos.

De manera oficial, dentro de la documentación del Sistema Integrado de Gestión en adelante SIG de la entidad, se cuenta con la Política de Administración de Riesgos, qué a través de la guía de administración de riesgos en el acápite N° 11 titulado IDENTIFICACIÓN Y GESTIÓN DEL RIESGO (RIESGO SEG. DE LA INFORMACIÓN) se determinan los lineamientos propios en esta materia, para así realizar la identificación de amenazas, vulnerabilidades, impactos, niveles de riesgos y tratamientos de los activos de información previamente identificados por todos los procesos; para tal fin la guía define las etapas que se deben desarrollar de manera dinámica y con esto lograr una adecuada gestión de riesgos.

Basado en lo mencionado y de acuerdo con el alcance del presente informe, a continuación, se describe para cada una de las etapas la gestión ejecutada por la Secretaría así:

4.1.1. Etapa 1: Conocimiento y divulgación:

En referencia a esta etapa se adelantaron las siguientes actividades:

- La segunda línea de defensa, en este caso la Dirección de Tecnologías y Sistemas de la Información en adelante **DTSI**, generó y remitió memorando interno a través del sistema de gestión documental SIGA con número 3-2024-42215 con asunto " *SOLICITUD CARGUE DE EVIDENCIAS A CONTROLES ESTABLECIDOS PARA ATENUAR LOS RIESGOS ASOCIADOS A SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN*. ", en el cual se solicita a las dependencias la carga de las evidencias correspondientes a los controles asociados a los riesgos de seguridad de la información, derivados de la gestión realizada en el último cuatrimestre de la vigencia 2024, definiendo la fecha límite.

- El día 19 de diciembre de 2024, la DTSI remite correo electrónico masivo a toda la entidad, socializando una pieza comunicativa y recordando el plazo para la carga de las evidencias de riesgos de seguridad de la información en el periodo comprendido entre el 1 al 9 de enero de 2025. En este mismo correo socializa la matriz oficial de riesgos de seguridad de la información. A continuación, se muestra la pieza gráfica remitida:

Imagen N° 1: Pieza comunicacional remitida por la DTSI a toda la entidad vía correo electrónico el día 19/12/2024. Fuente: INFORME TERCER CUATRIMESTRE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN - 2024 generado por la DTSI con radicado número 3-2025-1528 y correo electrónico enviado a todas las dependencias el día 19/12/2024.

- A manera de ejemplo, el día 30 de diciembre el contratista responsable por parte de la DTSI remite a cada proceso (Evaluación al Sistema de Control Interno (SM)) correo electrónico recordando el cargue de las evidencias. De acuerdo con lo indicado por el contratista en mención, este mismo ejercicio se realizó con todos los procesos.

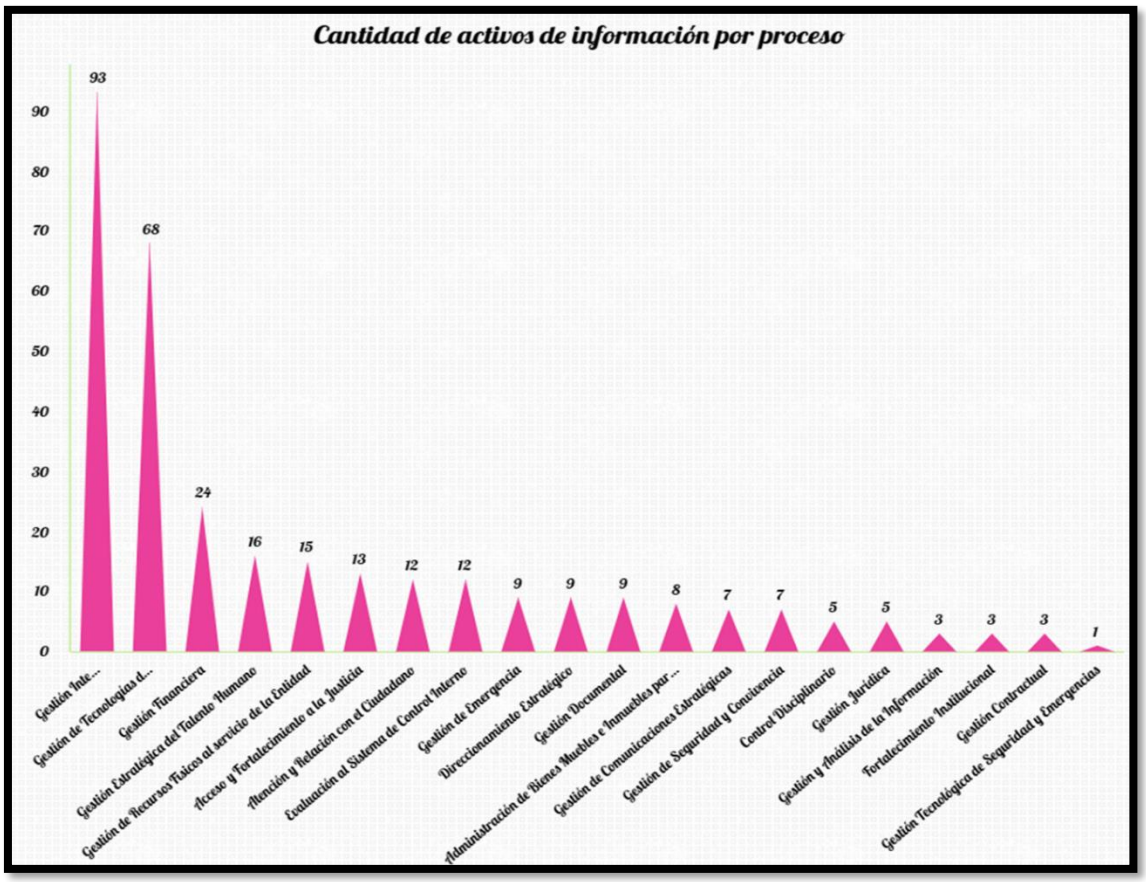
4.1.2. Etapa 2: Identificación de activos de seguridad de la información:

Una vez culminada la vigencia y de acuerdo a lo informado por la DTSI en el informe del tercer cuatrimestre riesgos de seguridad de la información – 2024, se obtuvo un nuevo total de **322** activos de información asociados a los procesos de la entidad, por consiguiente, se actualizó el registro de activos de información y el índice de información

clasificada y reservada de la entidad, que, en cumplimiento de la ley de transparencia, quedó publicada en el siguiente vinculo:

https://scj.gov.co/es/transparencia/datos-abiertos/registros-activos-informacion

La distribución por proceso de los activos de acuerdo con su criticidad se refleja de la siguiente manera:



Gráfica N° 1: Activos de información por proceso - Fuente matriz de riesgos de seguridad de la información F-FI-1385

Por lo informado, la entidad atendió la recomendación a lo descrito en la oportunidad de mejora N° 1 del informe correspondiente al cuatrimestre anterior, donde esta Oficina reportaba la falta de actualización del inventario de activos de información y el índice de información clasificada y reservada, ya que el último proceso se había suscitado en la vigencia 2022.

Finalmente, se validó con la DTSI acerca de la proyección y planeación de la actualización de activos de información para la vigencia 2025, a lo cual fue informado que se encuentra en proceso de definición de las fechas.

4.1.3. Etapa 3: Pasos para la identificación y/o valoración de activos:

La guía de administración de riesgos G-FI-04 V.3 indica en la etapa 3 que para la identificación y valoración de los activos de información se debe tener en cuenta las siguientes 8 variables:

1) Información del proceso.
2) Tipo documental.
3) Tipo de soporte.
4) Clasificación documental.
5) Clasificación y custodia de información.
6) Índice de información clasificada y reservada.
7) Infraestructura crítica cibernética.
8) Componente de seguridad de la información.

Para tal fin, se contrasta si estas variables se incluyeron en el registro de activos de información F-GD-1081 y la Matriz de Riesgos de Seguridad de la Información - 2024 F-FI-1385, así:

VARIABLE	DESCRIPCION	CUMPLE
Información del proceso	Cuenta con campos tales como ID, tipo de proceso, proceso, código el procedimiento y código del formato.	Si
Tipo documental	Para esta variable se identificaron los campos nombre del activo descripción del activo información e idioma.	Si
Tipo de soporte	Se definen campos como tipo de activo, descripción del soporte, formato y tipo de origen.	Si
Clasificación documental	se contemplan los campos serie, subserie y descripción	Si
Clasificación y custodia de la información	Se contemplan datos como la existencia de datos personales la clasificación de la información, custodio, estado, ubicación del activo, enlace de publicación en página web y propietario.	Si
índice de información clasificada y reservada	Se identifican campus tales como fecha de generación de la información clasificada, objetivo legítimo de la excepción, fundamento constitucional o legal, fundamento jurídico de la excepción excepción total o parcial, fecha de calificación y plazo de la clasificación o reserva.	Si
Infraestructura crítica cibernética	Pero es posible se discriminan 3 variables entre las cuales se mencionan impacto social, impacto económico e impacto ambiental	Si

VARIABLE	DESCRIPCION	CUMPLE
Componente de seguridad de la información	Se presentan 4 campos de confidencialidad, integridad, disponibilidad y criticidad o importancia del activo	Si

Tabla N° 1: - Elaboración propia - Variables para identificación y valoración de activos de información - Fuente: matriz de riesgos de seguridad de la información F-FI-1385.

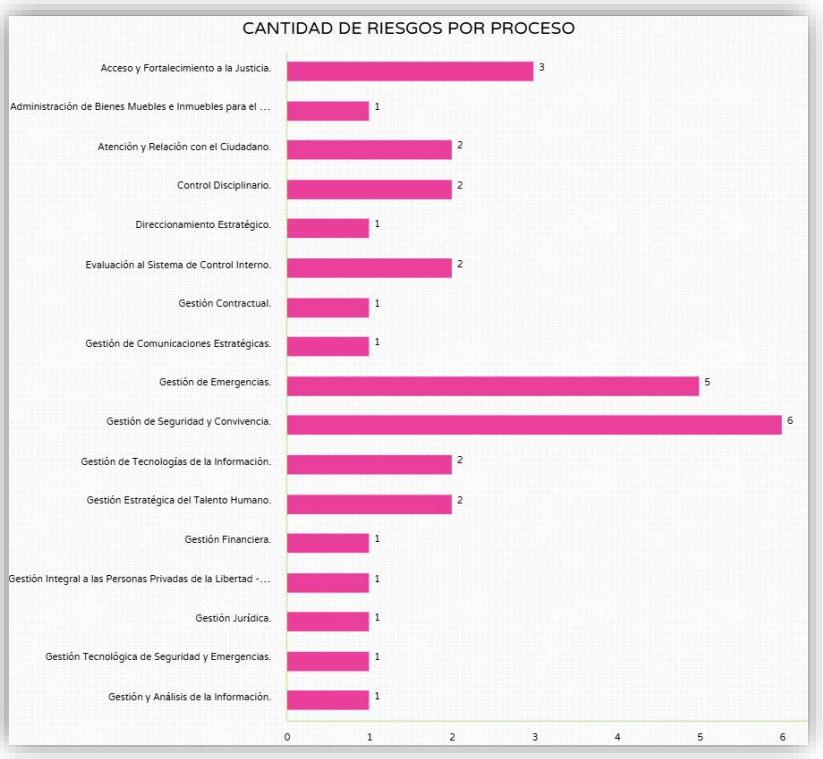
4.1.4. Etapa 4: Identificación del riesgo:

De acuerdo con la Guía de Administración de Riesgos G-FI-04 V.3 oficializada en el portal MIPG de la entidad, para esta etapa se podrán identificar 3 riesgos inherentes de seguridad de la información tales como **pérdida de la confidencialidad, pérdida de la integridad y pérdida de la disponibilidad.** A cada riesgo se debe asociar uno o varios ítems de activos de información del proceso y se analizan las amenazas y vulnerabilidades que podrían causar su materialización.

Ante lo descrito y revisando la matriz de riesgos de seguridad de la información de la entidad (F-FI-1385) con corte a 31 de diciembre de 2024, se reportan los siguientes elementos:

- 322 activos de información.
- 71 de los anteriores cuentan con calificación de criticidad Alta.
- 33 riesgos identificados analizados con amenazas, vulnerabilidades y consecuencias, con esto se establece el impacto y los riesgos inherentes.

Los 33 riesgos determinados y plasmados en la matriz de riesgos de seguridad de la información se presentan por proceso así:



Gráfica N° 2: elaboración propia; riesgos por procesos – Fuente: Matriz de riesgos de seguridad de la información 2024 F-FI-1385.

En referencia a esta etapa, esta Oficina resalta que en la vigencia 2024 se presentó un incidente relacionado con la documentación de la Unidad de Mediación – UMC en la Casa de Justicia de San Cristóbal, afectando físicamente los documentos y por tanto fueron eliminados por considerarse como pérdida total; está situación se detalla en el radicado N° 3-2024-26307 emitido por la Direccion de Recursos Físicos y Gestión Documental.

Al estimarse como una materialización de riesgos, desde sus roles la OCI expuso en la sesión de la Mesa Tecnica de Gobierno Digital con fecha 19 de noviembre de 2024 el caso, en donde de manera general se recomendó dar trámite a los lineamientos internos, es decir, desarrollar las actividades al materializarse un riesgo y catalogarse como incidente de seguridad de la información. Una vez expuesta esta situación y al observarse que dentro de la matriz de riesgos de seguridad de la información no se han adicionado ítems para el proceso de Gestión Documental (riesgos y controles), se presenta la siguiente oportunidad de mejora:

Oportunidad de Mejora N° 01: Falta de inclusión de riesgos y controles de seguridad de la información asociados al proceso de Gestión Documental, después de presentarse un incidente con documentos físicos en la casa de Justicia de San Cristóbal en la vigencia 2024.

Como se indicó en el párrafo anterior, se informa por parte de esta Oficina la no inclusión de riesgos y controles de seguridad de la información asociadas al proceso de Gestión Documental siendo que en la vigencia 2024 se presentó un incidente de destrucción de documentos sin el debido proceso, por tal razón, se recomienda continuar con el desarrollo de las actividades estipuladas dentro de la documentación del sistema integrado de gestión por parte de las dependencias involucradas e incluyéndolo también como incidente de seguridad de la información. De manera complementaria se sugiere reportar el avance de la gestión realizada en la siguiente mesa tecnica de Gobierno y Seguridad Digital.

Por otra parte, en el informe correspondiente al segundo cuatrimestre de 2024, fue informado por esta Oficina lo siguiente: *"Es de precisar que, si bien cada riesgo asocia un grupo de activos específicos por proceso, y sobre ellos se analizan las posibles amenazas, vulnerabilidades y consecuencias que podrían causar su materialización; no se observa de manera detallada cual es la homologación de los setenta y nueve (79) activos con Criticidad Alta con los veintisiete (27) riesgos identificados en la Matriz; por lo que, esta Oficina reitera las recomendaciones hechas en Informes anteriores, respecto a la revisión y homologación de los datos de Registro de Activos de Información e Índice de Información Clasificada y Reservada (F-GD-1081) con lo identificado en la Matriz de riesgos de seguridad de la información."*

La anterior situación continua en igual condición sobre la cual nos permitimos ampliar por medio de un ejemplo así:

El proceso de Acceso y Fortalecimiento a la Justicia cuenta con un total de 13 activos de información de los cuales 6 se catalogaron con criticidad alta así:

Información del Proceso					Tipo documental			Indice de Información	Infraestructura Critica Cibernética			Componente de Seguridad de la Información			
ID	Tipo de Proceso	Proceso	Código del Procedimiento	Código del Formato	Nombre del activo (Registro o documento de archivo)	Descripción del activo de información	Idioma	Plazo de la clasificación o reserv	Impacto Social	Impacto Económico	Impacto Ambiental	Confidencialidad	Integridad	Disponibilidad	Importancia del Activo / Criticidad del Activ
AI0239	Misionales	Acceso y Fortalecimiento a la Justicia	PD-AJ-10	NA	Registros de orientaciones y atenciones en Centros de Recepción e Información de Casas de Justicia	Corresponde a la base de datos que arroja el sistema de información institucional SIDUUS con el registro de orientaciones	Español	limitado	No	No	No	Alta	Alta	Alta	Alta
AI0240	Misionales	Acceso y Fortalecimiento a la Justicia	PD-AJ-10	NA	Registros de orientaciones y atenciones en Unidades Móviles de Acceso a la Justicia	Corresponde a la base de datos que arroja el sistema de información institucional SIDUUS con el registro de orientaciones	Español	limitado	No	No	No	Alta	Alta	Alta	Alta
AI0241	Misionales	Acceso y Fortalecimiento a la Justicia	PD-AJ-10	NA	Registros de orientaciones en canales no presenciales de Casas de Justicia	Corresponde a la base de datos que arroja el sistema de información institucional SIDUUS con el registro de orientaciones	Español	limitado	No	No	No	Alta	Alta	Alta	Alta
AI0242	Misionales	Acceso y Fortalecimiento a la Justicia	PD-AJ-10	NA	Registros de orientaciones y atenciones en Unidades de Mediación y Conciliación	Corresponde a la base de datos que arroja el sistema de información institucional SIDUUS con el registro de orientaciones	Español	limitado	No	No	No	Alta	Alta	Alta	Alta
AI0243	Misionales	Acceso y Fortalecimiento a la Justicia	PD-AJ-10	NA	Registros de orientaciones de la estrategia de facilitadores de acceso a la	Corresponde a la base de datos que arroja el forms institucional con el registro de orientaciones	Español	limitado	No	No	No	Alta	Alta	Alta	Alta
AI0249	Misionales	Acceso y Fortalecimiento a la Justicia	N/A	N/A	Bases de datos información operativa de los programas y estrategias DRPA	Corresponde a bases de datos en Excel (Office 365) que contienen datos sociodemográficos de las personas remitidas y vinculadas, datos asociados al proceso penal, registros de atenciones realizadas por los equipos interdisciplinarios según la asignación.	Español	limitada	No	No	No	Alta	Alta	Media	Alta

Imagen N° 2: Listado activos de información con valoración alta correspondientes al Proceso y Acceso y Fortalecimiento a la Justicia – Fuente F-FI-1385_Matriz de Riesgos de Seguridad de la Información - 2024 Hoja LISTADO DE ACTIVOS - ICC

Esta imagen lista los siguientes activos de información:

- Registros de orientaciones y atenciones en Centros de Recepción e Información de Casas de Justicia.
- Registros de orientaciones y atenciones en Unidades Móviles de Acceso a la Justicia.
- Registros de orientaciones en canales no presenciales de Casas de Justicia.
- Registros de orientaciones y atenciones en Unidades de Mediación y Conciliación.
- Registros de orientaciones de la estrategia de facilitadores de acceso a la justicia.
- Bases de datos información operativa de los programas y estrategias DRPA.

En la hoja RIESGOS INHERENTE de la Matriz de Riesgos de Seguridad de la Información - 2024 se identifican los siguientes activos asociados a 3 riesgos del proceso de acceso y fortalecimiento a la justicia así:

IDENTIFICACIÓN DE RIESGOS									
RIESGO	PROCESO	ACTIVO	RIESGO	AMENAZA	VULNERABILIDAD	CONSECUENCIA	PROBABILIDAD	IMPACTO	RIESGO INHERENTE
1	Acceso y Fortalecimiento a la Justicia.	Documentación DAJ (Plan de Acción de Casas de Justicia,Actas del Comité de Coordinación Local de las Casas de Justicia,Acciones Preventivo – Pedagógicas, Seguimiento a la Implementación del Traslado por Protección y Atención Psicológica a la Población Trasladada, Historias de Procesos de Mediación para la Solución de Conflictos, Base de datos Historias del programa de justicia juvenil restaurativa, expedientes Historias del programa de justicia juvenil restaurativa, Acuerdos de ingreso y convivencia Programa De Seguimiento Judicial al Tratamiento de Drogas, Consentimiento Informado Mayor de Edad, Consentimiento Informado Menor de Edad, Informe De Seguimiento Programa De Seguimiento Judicial al Tratamiento de Drogas, Informe Extraordinario Programa De Seguimiento Judicial al Tratamiento de Drogas , Informe Final PSJTD, Valoración Inicial del Programa De Seguimiento Judicial al Tratamiento de Drogas, Visita Domiciliaria, Equipo Psicosocial. PSJTD, BD PSJTD)	Pérdida de la Confidencialidad	Error en el uso	Ausencia de documentación.	Pérdida o detrimento de información	Baja	Moderado	MODERADO
2	Acceso y Fortalecimiento a la Justicia.	Formularios (Formulario de forms registro atenciones virtuales Centro de Recepción e Información CRI, Formulario de forms registro jornadas unidades móviles para el acceso a la justicia, Formulario forms encuesta de satisfacción Dirección de Acceso a la Justicia)	Pérdida de la Confidencialidad	Abuso de derechos.	Asignación errada de los derechos de acceso.	Pérdida o detrimento de información	Baja	Moderado	MODERADO
3	Acceso y Fortalecimiento a la Justicia.	Bases de datos información operativa de los programas y estrategias DRPA	Pérdida de la Integridad.	Error en el uso	Ausencia de copias de respaldo.	Pérdida o detrimento de información	Baja	Leve	BAJA

Imagen N° 3: Listado activos de información del Proceso Acceso y Fortalecimiento a la Justicia – Fuente F-FI-1385_Matriz de Riesgos de Seguridad de la Información - 2024 Hoja LISTADO DE ACTIVOS - ICC

Con los siguientes activos de información:

a) Documentación DAJ (Plan de Acción de Casas de Justicia, Actas del Comité de Coordinación Local de las Casas de Justicia, Acciones Preventivo – Pedagógicas, Seguimiento a la Implementación del Traslado por Protección y Atención Psicológica a la Población Trasladada, Historias de Procesos de Mediación para la Solución de Conflictos, Base de datos Historias del programa de justicia juvenil restaurativa, expedientes Historias del programa de justicia juvenil restaurativa, Acuerdos de ingreso y convivencia Programa De Seguimiento Judicial al Tratamiento de Drogas, Consentimiento Informado Mayor de Edad, Consentimiento Informado Menor de Edad, Informe De Seguimiento Programa De Seguimiento Judicial al Tratamiento de Drogas, Informe Extraordinario Programa De Seguimiento Judicial al Tratamiento de Drogas , Informe Final PSJTD,

Valoración Inicial del Programa De Seguimiento Judicial al Tratamiento de Drogas, Visita Domiciliaria, Equipo Psicosocial. PSJTD, BD PSJTD).

b) Formularios (Formulario de forms registro atenciones virtuales Centro de Recepción e Información CRI, Formulario de forms registro jornadas unidades móviles para el acceso a la justicia, Formulario forms encuesta de satisfacción Dirección de Acceso a la Justicia).

c) Bases de datos información operativa de los programas y estrategias DRPA.

Con base en la diferencia de datos/ítems de activos de información registrados en la matriz se riesgos de seguridad de la información, se presenta la siguiente oportunidad de mejora:

Oportunidad de Mejora N° 02: Falta de concordancia en los activos de información dentro Formato F-GD-1081 Registro de Activos de Información y la Matriz de Riesgos de Seguridad de la Información:

Se observaron diferencias de activos de información registrados en la matriz de riesgos de seguridad de la información F-FI-1385_Matriz, entre lo listado en la columna REGISTRO DEL ACTIVO hoja LISTADO DE ACTIVOS – ICC versus la columna ACTIVO de la hoja RIESGO INHERENTE, puesto que en una se presentan 6 ítems y en la otra 3 de manera consolidada, pero sin tener concordancia contra el primero (Lo anterior respecto al proceso Acceso y Fortalecimiento a la Justicia).

De igual manera, se insta a la segunda línea de defensa a realizar una revisión detallada y actualización de los activos de información de TODOS los procesos, de acuerdo con la metodología de la entidad, los cuales deben ser consistentes y coherentes dentro del instrumento establecido para tal fin.

Por otro lado, en la matriz de riesgos de seguridad de la información se detalla un listado de amenazas vinculadas a cada uno de los riesgos identificados y clasificados.

Al contrastar este listado con las amenazas comunes que podrían impactar los activos de la entidad, según lo establecido en la guía de administración de riesgos G-FI-04 V.3, se observa que estas no han sido incorporadas en la guía en mención. A continuación, se presentan los siguientes ejemplos:

- Incumplimiento de la Divulgación.
- Indisponibilidad del sistema de información.
- Fenómenos Ambiental.
- Perdida de Información.
- Actividad Maliciosa de Ciberdelincuente.
- Gestión Inadecuada de la Información.

- Ciberataque.
- Modificación de bases de datos.
- Uso no autorizado de credenciales de administración a cualquiera de los componentes de la infraestructura de la SDSCJ.
- Ciberataque o incidente informático a la infraestructura del proveedor de nube.
- Ciberataque dirigido a la infraestructura de la Entidad.

Por lo anterior, se presenta la siguiente oportunidad de mejora:

Oportunidad de Mejora N° 03: Falta de consistencia entre los listados de amenazas descritos en la guía de administración del riesgo y la matriz de riesgos de seguridad de la información del SIG de la entidad:

Como se mencionó, dentro de la matriz de riesgos de seguridad de la información F-FI-1385_Matriz se listan una serie de amenazas en materia de seguridad de la información, las cuales no se han catalogado en la guía administración de riesgos de la entidad, resaltando que las guías sirven como documentos de referencia que proporciona directrices claras y detalladas sobre cómo implementar, operar, mantener y mejorar el sistema de gestión; de acuerdo con esto, se sugiere a la segunda línea de defensa realizar una validación y actualización de lo que actualmente se encuentra registrado en la matriz de riesgos de seguridad de la información, versus la teoría descrita en la guía de administración de riesgos en el acápite de seguridad de la información, a fin de tener coherencia entre los 2 elementos.

4.1.5. Etapa 5: Valoración del riesgo:

Dentro de la matriz de riesgos de seguridad de la información, para los 33 riesgos catalogados y una vez registradas las amenazas, las vulnerabilidades y las consecuencias, la entidad procedió a calificar la probabilidad y el impacto para así obtener como resultado el riesgo inherente.

Como resultado se obtienen 5 riesgos en nivel alto, 28 riesgos en nivel moderado y 2 riesgos en nivel bajo. Cabe aclarar que la sumatoria de estos 3 niveles no es 33 debido a que por la cantidad de vulnerabilidades identificadas es posible que para un mismo riesgo se haya identificado y/o catalogado los 3 niveles bajo, medio y alto (ver tabla N° 2 celdas con color amarillo), por tanto, la cantidad total de registros reportados son 43.

A continuación, se presenta la valoración de los riesgos de seguridad de la información en la entidad:

Valoración Riesgo Inherente	Numero de riesgo																															Totales
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	
ALTO				1					1																2	2							1	7
BAJA			1	1																														2
MODERADO	1	1		2	1	1	1	1		2	1	1	1	3	1	1	1	1	1	2	1	1	1	1			1	1	1	1	1	2		34
Total	1	1	1	4	1	1	1	1	1	2	1	1	1	3	1	1	1	1	1	2	1	1	1	1	2	2	1	1	1	1	1	2	1	43

Tabla N° 2: - Elaboración propia – Valoración de riesgos de seguridad de la información - Fuente: matriz de riesgos de seguridad de la información F-FI-1385.

4.1.6. Etapa 5: Creación de controles:

La guía de administración de riesgos en el numeral 9.7 titulada creación de controles, describe los lineamientos para la estructuración de estos de la siguiente manera:

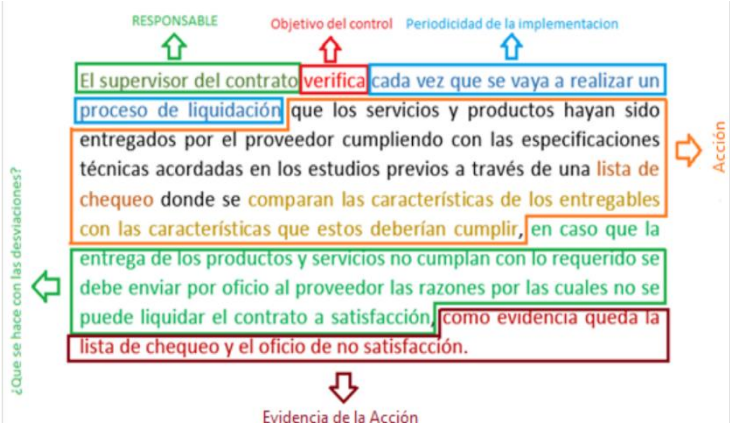


Imagen N° 4: Estructura para la construcción de un control. Fuente: Guía de administración de riesgos numeral 9.7

A corte 31 de diciembre de 2024, dentro la matriz de riesgos de seguridad de la información en la hoja titulada TRATATAMIENTO DEL RIESGO, se tienen catalogados 43 controles asociados a los 33 riesgos. Los campos de información que contiene la matriz para el tema de controles son:

- Proceso: Describe el nombre del proceso de acuerdo con el mapa de procesos de la entidad.
- Número de control: numeración consecutiva de los controles de acuerdo con los riesgos por cada uno de los procesos.
- Tipo de acción: para este campo se pueden seleccionar 4 opciones aceptar, reducir, evitar y compartir el riesgo.
- Causa mitigada: Describe la vulnerabilidad previamente identificada.

- Consecuencias mitigadas: Reporta las consecuencias previamente analizadas y catalogadas dentro de la fase identificación de riesgos.
- Descripción del control: Describe el control de acuerdo con la estructura presentada en la imagen N°4 para cada uno de los procesos.
- Tipo de control: En este campo se pueden catalogar 2 opciones, preventivo o detective.
- Responsable del control: El campo permite identificar si el control tiene asignación o no de responsable.
- Responsable de implementación adecuado: Identifica si el responsable de la implementación es adecuado o no.
- Evidencia la ejecución del control: El campo permite catalogar si la evidencia es completa, incompleta o no existe.
- Fuente de información confiable para el desarrollo del control: Identifica si la fuente de información es o no confiable.
- Desviaciones son resueltas de manera oportuna: El campo permite seleccionar si las desviaciones se investigan o no se investigan.
- Periodicidad de la aplicación de controles adecuada: Campo que permite registrar si la periodicidad determinada es adecuada o no.
- Indicador: registras y el ítem cuenta con indicadores, para el caso de la matriz de riesgos, todos los registros cuentan con valor no aplica.

Complementariamente la matriz cuenta con una sección para el diligenciamiento por parte del administrador del riesgo de la segunda línea, conteniendo los siguientes campos:

- Evaluación del control: Valor numérico producto de la evaluación del control.
- Calificación del diseño de control: Cuenta con 3 valores, fuerte, moderado o débil dependiendo la evaluación del control.
- Calificación de la implementación: de acuerdo con la calificación de la implementación se pueden clasificar en fuerte, moderado o débil.
- Solidez individual del control plan de acción para fortalecer el control: de igual manera y de acuerdo con la calificación se puede clasificar en fuerte, moderado o débil
- Observaciones: el campo funciona para registrar observaciones en caso de que aplique; para la matriz de riesgos de seguridad de la información en la totalidad de esta columna se registra el valor no aplica.

En otra medida y de acuerdo con el informe remitido por la DTSI para el presente corte y en concordancia con las recomendaciones emitidas por esta Oficina en el informe correspondiente al segundo cuatrimestre de 2024, en el cual se indicaba qué: " *es importante que la 1LD y 2LD verifiquen en la descripción de los controles, si la acción establecida es coherente con la evidencia de la acción y el objetivo del control. De igual*

forma, y según lo previsto en el antedicho documento: "La definición del control debe incluir en que situaciones se presentan desviaciones entre el resultado esperado y el resultado obtenido y que acciones se deben tomar si se presentan dichas desviaciones" (negrilla fuera de texto); se recomienda revisar los controles en donde la variable desviación no obedece a lo citado en la guía. "; en consecuencia, de lo anterior, se presentaron actualizaciones y/o ajustes a controles para los siguientes procesos:

- ✓ **Evaluación al sistema de control interno**: Riesgo 10 control 1: El profesional de la Oficina de Control Interno de forma trimestral descarga el reporte del sistema de información con el estado de los planes de mejoramiento institucional y procede a cargar el archivo en el repositorio SharePoint disponible para la Oficina de Control Interno. En caso de no poder descargar el reporte se solicita a la Dirección de Tecnologías y Sistemas de la Información se genere el reporte correspondiente por parte del administrador de la herramienta.

- ✓ **Acceso y fortalecimiento a la justicia**: Riesgo 2 control 1. El profesional y/o los profesionales de la dirección de acceso designados para esta actividad trimestralmente solicita la verificación de los permisos de derecho de acceso a los diferentes formularios, de acuerdo con los roles y responsabilidades asignados para tal fin, como soporte de la revisión enviará este profesional comunicación oficial y/o correo electrónico a los responsables del área solicitando esta información, en caso que los usuarios no tengan autorización se retiraran permisos de acceso y se informara de las acciones al Jefe de área.

- ✓ **Gestión de Emergencias**: Riesgo 14 control 1. El responsable del proyecto NUSE123, de forma mensual verifica los informes de seguimiento a la operación entregados por el operador tecnológico y los informes de interventoría del cumplimiento aprobados para los tramites de pagos correspondientes. como evidencia se entregan los informes de seguimiento a la operación, informe de interventoría y el informe de supervisión del mes vencido, En caso de no contar con los reportes que entrega el operador tecnológico, se realizaran las gestiones pertinentes mediante comunicado oficial y/o correo electrónico sobre la solicitud de información. El cargue de las evidencias se hará de forma cuatrimestral.

- ✓ **Gestión de Emergencias:** Riesgo 15 control 1. El grupo de seguimiento de infraestructura tecnológica del C4, realizan la verificación de acciones preventivas y correctivas a UPS y Planta eléctrica programados en el contrato de mantenimiento establecido por parte de la Secretaría Distrital de Seguridad, convivencia y Justicia. Como evidencia se cargan los informes técnicos de funcionamiento de las UPS, en caso de no realizar los mantenimientos programados se deberá informar mediante correo electrónico sobre los motivos, así como las acciones para cumplir con los mantenimientos. el cargue de evidencia se hará trimestralmente.

- ✓ **Gestión de Seguridad y Convivencia**: Riesgo 23 control 1. El responsable de gestión de la información de la Subsecretaría de Seguridad y Convivencia verifica semestralmente, que todos los registros del formulario sean actualizados al menos una vez por cada vigencia esto se evidencia mediante los datos del formulario con las fechas de actualización para cada registro. En caso de no realizar la actualización completa los registros pendientes se sumarán a la meta de actualización del siguiente periodo.

- ✓ **Gestión Tecnológica de Seguridad y Emergencias**: Riesgo 32 control 1. El supervisor del contrato de mantenimiento de video vigilancia y los profesionales de apoyo al mismo, realizan seguimiento a los mantenimientos de los equipos que conforman el sistema de video vigilancia, como evidencia se debe presentar el reporte mensual de los mantenimientos realizados avalado por la interventoría y/o supervisión acompañado de la conciliación técnica mensual de ANS aplicados al contratista, mes vencido, en caso de no contar con los reportes que entrega el contratista, se realizaran las gestiones pertinentes mediante comunicado oficial y/o correo electrónico sobre la información. El cargue de las evidencias se consolidará de forma cuatrimestral.

- ✓ **Gestión Tecnológica de Seguridad y Emergencias**: Riesgo 32 control 2. El jefe del C4 supervisa a la empresa contratista del mantenimiento del sistema de video vigilancia y garantías extendidas del Centro de Computo. Estas actividades se registran en los informes de gestión de la empresa contratista, los cuales son recibidos y estos a su vez evidencian la operación del sistema de video vigilancia controlada por ANS, que en caso de estar por debajo de umbral se penaliza económicamente. Las evidencias corresponden al Informe mensual de la empresa contratista e informe de seguimiento mensual del contrato que se allega al mes vencido. El cargue de las evidencias se hará de forma cuatrimestral.

Una vez descritos los controles actualizados, se identifica por parte de la OCI que la recomendación fue acogida en el sentido en que estos cuentan con la inclusión de las desviaciones y las acciones que se deben tomar si se presentan.

Por otra parte, sobre esta etapa la guía indica que un control sea adecuado en su diseño y que su implementación sea efectiva a la hora de mitigar un riesgo, se crea de acuerdo con los lineamientos descritos en el numeral 9.7 del documento. Ahora bien, en el numeral 9.7.2 titulado ***tipos de controles***, se define la existencia de 3 tipos de controles a saber, preventivos, detectivos y correctivos, tema contenido dentro de la matriz de riesgos de seguridad de la información en la hoja TRATAMIENTO DE RIESGO; no obstante, a lo anterior, se resalta que el numeral indica también la existencia de otras tipologías correspondientes a cómo se ejecuta el control, es decir su implementación, así:

- Controles manuales: Ejecutados por personas.
- Controles automáticos: Ejecutados por un sistema.

Como tal, se informa que la matriz de riesgos de seguridad de la información no contiene esta catalogación de controles, por tanto, se presenta la siguiente oportunidad de mejora:

Oportunidad de Mejora N° 04: Falta de inclusión de tipologías de controles automáticos y manuales en la estructuración de estos dentro de la matriz de riesgos de seguridad de la información.

Cómo se indicó, la matriz de riesgos de seguridad de la información para los controles identificados no contiene las tipologías asociadas al cómo se ejecuta el control, tales como controles **manuales y automáticos**, descritos en el numeral 9.7.2 de la guía de administración de riesgos G-FI-04 V.3 de la entidad. Por lo anterior, se aconseja sea evaluada de manera integral para todos los controles y entre las diferentes líneas de defensa, la inclusión de estos atributos, para así alinear estos con lo descrito en la guía de la entidad.

4.1.7. Etapa 7: Tratamiento del riesgo residual.

La guía de administración de riesgos indica que para los riesgos de seguridad de la información y dada la zona de riesgo residual obtenida con la ejecución de los controles se realizará un tratamiento de riesgos identificados bajo las siguientes tipologías:

- Aceptar el riesgo.
- Reducir el riesgo
- Evitar el riesgo
- Compartir el riesgo.

Como tal, dentro de la matriz de riesgos de seguridad de la información en la hoja TRATAMIENTO DE RIESGO RESIDUAL, la totalidad de controles, es decir 43 obtuvieron como valoración y catalogación final el ítem **reducir el riesgo**.

4.1.8. Etapa 8: Monitoreo, revisión y reporte.

Para esta etapa, la guía de administración de riesgos indica que, se debe hacer de manera permanente evaluación para asegurar que la gestión de los riesgos se está llevando a cabo bajo los aspectos y lineamientos definidos en materia de seguridad de la información, por tanto, se definen 5 variables así:

Aspecto	Comentario OCI
El Mapa de riesgos de seguridad de la información, debe contener aquellas acciones de control definidas para el manejo del riesgo, buscando prevenir o reducir el riesgo detectado, teniendo en cuenta su viabilidad técnica y financiera. El monitoreo de las acciones de tratamiento debe realizarlo el responsable del proceso	La matriz de riesgos de seguridad de la información contiene dentro de los controles acciones relacionadas para el tratamiento del riesgo, no obstante, como se indicó en el numeral 4.1.6 del presente informe y alineándose a lo establecido en el numeral 9.7 de la guía, es importante catalogar las tipologías de controles tales como manuales y automáticos esto, con el fin valorar y fortalecer el control. En la parte final de este aspecto se menciona que el monitoreo debe realizarlo el responsable del proceso, no obstante, dentro de la documentación y/o evidencias relacionadas con seguridad de la información, no se identifica el monitoreo que realiza el responsable del proceso, por lo anterior, se sugiere sea validada la ejecución de esta actividad por parte de la segunda línea de defensa y si el caso aplica, ajustar la política de administración de riesgos.
El responsable del proceso debe verificar que los controles establecidos en la matriz de riesgos operen de manera adecuada para mitigar los riesgos.	Cómo se mencionó en el aspecto anterior, no se identifica la revisión que hace el responsable del proceso a los controles establecidos en la matriz, por tanto, se recomienda sea validada esta actividad de la política de administración de riesgos conjuntamente entre la primera y segunda línea de defensa.
El seguimiento de los riesgos identificados (incluyendo el tratamiento) se debe realizar de manera cuatrimestral por cada uno de los líderes de los procesos, quienes reportarán a la Dirección de Tecnologías y Sistemas de la Información quien consolidará y posteriormente enviará a la Oficina Asesora de Planeación para su publicación	Para el presente seguimiento se identifica la generación de las evidencias por parte de cada uno de los procesos asociados a los riesgos y controles. A su vez, la DTSI (segunda línea de defensa) consolidó la información y generó el informe de seguimiento de acuerdo con su revisión.
Anualmente se debe realizar la valoración de los riesgos de seguridad de la información con el fin de verificar que el tratamiento fue efectivo y los niveles de riesgo disminuyeron	En el numeral 5 del informe emitido por la DTSI el cual titula análisis de la matriz de riesgos, se informa que: "*Todas las valoraciones se realizaron de parte de los Líderes de proceso o los Líderes Operativos en compañía de sus grupos de trabajo, contando con el acompañamiento y orientación de la Dirección de*

Aspecto	Comentario OCI
	Tecnologías y Sistemas de la Información, dichas valoraciones de Probabilidad e Impacto nos dan como resultado la Zona de Riesgo Inherente", complementándose con "*Dada la necesidad de dar trámite y continuidad a los procedimientos y actividades establecidos por los procesos, para ninguno de los riesgos identificados se determinó "Evitar" como medida de tratamiento para el riesgo. Contrario a ello se optó por "Reducir el riesgo" como la medida por los procesos, con esto se hace necesaria la ejecución de controles para minimizar posibilidad de materialización de los riesgos, en concordancia con lo establecido en la Política de Administración de Riesgos de la Entidad.".* Por lo anterior, este aspecto fue cumplido en la vigencia 2024.
El responsable de realizar el seguimiento a los riesgos de seguridad de la Información debe reportar cuatrimestralmente a la mesa técnica de Seguridad Digital.	En la última sesión de la mesa técnica de gobierno digital realizada en la vigencia 2024, fueron reportados los avances respecto a riesgos de seguridad de la información y seguridad digital, de acuerdo con el lineamiento de esta fase, es decir, se cumplió con lo establecido.

Tabla N° 3: - Elaboración propia – Fuente: guía de administración de riesgos G-FI-04 V.3.

4.2. Seguimiento a la Ejecución de controles.

Para el seguimiento y evaluación de la ejecución de los controles definidos en la Matriz de Riesgos de Seguridad de la SDSCJ, la Oficina de Control interno verificó los soportes allegados por la primera línea de defensa sobre el repositorio que la segunda línea de defensa (DTSI) tiene para tal fin y como resultado se obtuvo lo siguiente:

Riesgo	Proceso	Control	Evidencia o soporte visualizado	Seguimiento OCI febrero 2025	Cumple
1	Acceso y Fortalecimiento	1	Archivo informe de gestión 2024.	En el seguimiento anterior realizado por la OCI se indicó: " *en la descripción del Control no hay claridad ni especificación de la evidencia de la acción, por lo cual no es posible determinar si el proceso aportó la evidencia idónea para la ejecución del control.* "	No

Riesgo	Proceso	Control	Evidencia o soporte visualizado	Seguimiento OCI febrero 2025	Cumple
	a la Justicia.			Para el presente seguimiento se informa que el control continúa en las mismas condiciones, sin haber recibido una actualización.	
2	Acceso y Fortalecimiento a la Justicia.	1	• Correo solicitando reporte de información. • Correo validación de forms. • Matriz de reportes de la dirección de acceso a la justicia	El correo de validación de forms tiene fecha 21/08/2024, De acuerdo con lo indicado por el control, este se debe generar trimestralmente por tanto se presenta incumplimiento para el presente seguimiento. Adicionalmente, no se observa si se hizo una revisión o depuración de usuarios de acuerdo a la parte final del control el cual indica que " *en caso de que los usuarios no tengan autorización se retiraran permisos de acceso y se informara de las acciones al Jefe de área*. "	No
3	Acceso y Fortalecimiento a la Justicia.	1	• Correo de reporte plan de ejecución de copias. • Reporte plan de copias. • Plan de copias de respaldo	Este control es nuevo y comienza su operación a partir del mes de diciembre de 2024; el equipo auditor identifica el cumplimiento de la ejecución del control de acuerdo con lo establecido, puesto que se reporta al Director de la dependencia el estado de ejecución de las copias de seguridad de la información a través de un informe remitido vía correo electrónico.	Si
4	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	1	Correo electrónico titulado seguridad de la información tics	El control indica: "*como evidencia se entrega el reporte mensual de fallas de producción el cual se solicitará mediante correo electrónico y/o comunicado oficial a la DTSI. en caso de no entregar el reporte se debe informar al director de Bienes con las acciones para dar cumplimiento*. "; dentro de los soportes entregados solamente se encuentra el correo electrónico donde la Dirección de Bienes solicita a la DTSI el reporte de estado del sistema de información SIMBA, sin embargo, no se evidencia la respuesta con el reporte de estado del sistema por parte de la DTSI, ni el correo electrónico donde se informa al Director de Bienes que el reporte no fue recibido.	No
4	Administración	2	Correos remitiendo los	Si bien el control se está ejecutando tal como está establecido en el cual se informa a los diferentes	No

Riesgo	Proceso	Control	Evidencia o soporte visualizado	Seguimiento OCI febrero 2025	Cumple
	de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.		accesos y solicitando el cambio de contraseñas a los talleres que ingresan al sistema de información SIMBA.	talleres sobre el acceso a al sistema de información SIMBA y recordando el cambio de contraseña, el indicado control menciona que esto se debe realizar de manera mensual, al revisar los soportes remitidos por la dependencia responsable, se identifica que por ejemplo para Hyundai autos se relacionó soporte correspondiente para el mes de octubre y para el mes de diciembre quedando faltante el soporte del mes de noviembre de 2024, por tal motivo se recomienda a la primera y segunda línea de defensa ser exhaustivo tanto en la aplicación como en la revisión del control.	
4	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	3	3 actas de capacitación a los Talleres Hyundai, grupo de movilidad y AutoCars	Para el presente seguimiento, se remitieron dentro del repositorio dispuesto por la DTSI 3 actas de capacitación realizadas, sin embargo, no se identifican capacitaciones realizadas a grupo Morarci, UMG – Honda, Invercol Toyota, Jako Importaciones y Moto Speed Suzuki entre otros terceros. Por lo anterior, se indica que el control no se está ejecutando para todos los actores relacionados con el sistema de información SIMBA, para lo cual se insta a remitir los soportes de manera cuatrimestral, tal como lo estipula el control.	No
4	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades	4	Correo electrónico indicando la necesidad de personal para el sistema de información SIMBA.	De acuerdo a la validación realizada, el control se está ejecutando de acuerdo a lo establecido puesto que se está informando al Director de Bienes las necesidades de personal que requiere el sistema de información SIMBA, en este caso para la vigencia 2025.	Si

Riesgo	Proceso	Control	Evidencia o soporte visualizado	Seguimiento OCI febrero 2025	Cumple
	Operativas.				
5	Atención y Relación con el Ciudadano.	1	Soportes correspondientes a los meses de agosto, septiembre, octubre y noviembre con las matrices de MATRIZ DE TRAZABILIDAD DE PQRSDF CIUDADANAS Formato 1478	Al validar las evidencias cargadas al repositorio de la DTSI (segunda linea de defensa) por parte del proceso responsable, el control se encuentra ejecutándose correctamente, debido a que se remite la matriz de trazabilidad de PQRSDF.	Si
6	Atención y Relación con el Ciudadano.	1	2 reportes en Excel donde se encuentran los usuarios registrados tanto de abogados como funcionarios	Si bien se evidencian los listados de usuarios del sistema, el control apunta a la solicitud que se realiza a la DTSI solicitando el envío de la información ("*como soporte de la revisión enviara correo electrónico y/o comunicación vía Teams solicitando él envió de información y la respuesta requerida al personal encargado, en caso que exista usuarios no autorizados se solicita retirar los permisos de acceso e informar las actividades realizadas*"), aspectos que no se visualizan; por lo indicado, se recomienda realizar revisión del control actualmente estipulado con los soportes que se deben ejecutar por parte de la primera y segunda línea de defensa.	No
7	Control Disciplinario.	1	2 soportes otorgando los accesos.	Se identifican 2 soportes de correo electrónicos con solicitudes tramitadas al interior de control interno disciplinario en el mes de diciembre de 2024, por tanto, se concluye que el control está ejecutandose correctamente tal como lo indica su descripción.	Si
8	Control Disciplinario.	2	Correo electrónico.	Dentro del correo electrónico remitido, se observa el reporte de los usuarios actualmente autorizados y la aprobación por parte del Jefe de la Oficina Control Interno Disciplinario, por lo anterior, el control se está ejecutando correctamente.	Si
9	Direccionamiento Estratégico.	1	• Matriz Índice de transparencia y acceso a la información.	La Oficina Asesora de Planeación remite a las dependencias responsables correos de alertamiento respecto a la publicación de información en el sitio web, no obstante, el control indica: " *Como evidencia quedara el correo de notificación y el esquema de*	No

Riesgo	Proceso	Control	Evidencia o soporte visualizado	Seguimiento OCI febrero 2025	Cumple
			• correos electrónicos alertando a las dependencias la publicación de información en la página web.	*publicación*." y una vez revisada la documentación, no se evidencia el esquema de publicación, razón por la cual se recomienda tanto al responsable del control como a quien ejecuta el monitoreo, revisar detalladamente lo escrito en este para así generar las evidencias correspondientes.	
10	Evaluación al Sistema de Control Interno.	1	3 solicitudes de acceso a la herramienta de planes de mejoramiento de la Contraloría de Bogotá.	El control fue actualizado por la Oficina de Control Interno en el mes de diciembre de 2024; complementariamente y de cara al corte del seguimiento, por las evidencias presentadas el control se ejecutó correctamente.	Si
10	Evaluación al Sistema de Control Interno.	2	1 memorando.	Se evidencia memorando con radicado número 3-2024-9876, generado por la Oficina de Control Interno en el cual se socializa a todas las dependencias la actualización del procedimiento del plan de mejoramiento de la contraloría, así como se invita a los enlaces de cada dependencia a las sesiones de socialización. Por lo identificado, el control se encuentra operando correctamente.	Si
11	Evaluación al Sistema de Control Interno.	1	Reporte sistema ITS con corte a 31/12/2024.	El control se encuentra operando correctamente debido a que como evidencia se remite el reporte del sistema ITS con el listado de todos los planes de mejoramiento interno y dentro de las fechas establecidas. REVISAR CON KAROL	Si
12	Gestión Contractual.	1	Formato FUID 2024	Se identifica el formato FUID de contratos y convenios pertenecientes a la Dirección Jurídica de la vigencia 2024 tal y como lo establece el control por tal razón, se indica que este se encuentra operando correctamente.	Si
13	Gestión de Comunicaciones Estratégicas.	1	Correos electrónicos y evidencias de cambio de contraseña en las redes sociales de la entidad	El control se encuentra operando de acuerdo a lo establecido en la matriz de riesgos de seguridad de la información, debido a que la dependencia responsable remite soportes donde permite evidenciar los procesos de cambios de contraseñas de las redes sociales de la entidad.	Si
14	Gestión de Emergencias.	1	7 informes	El proceso responsable remite 3 informes de gestión y operación correspondientes a los meses de septiembre, octubre y noviembre, así como también 2 informes de interventoría y finalmente 2 informes	Si

Riesgo	Proceso	Control	Evidencia o soporte visualizado	Seguimiento OCI febrero 2025	Cumple
				de supervisión correspondientes a los meses de septiembre y octubre. El control se está cumpliendo de acuerdo a lo establecido, no obstante, se enfatiza en el cumplimiento y adición de los soportes correspondiente del cuatrimestre evaluado, ya que por ejemplo para los informes de supervisión está pendiente la carga del soporte correspondiente al mes de noviembre de 2024, así como el informe de gestión y operación de ETB.	
14	Gestión de Emergencias.	2	Correos semanales de proyección de personal desde septiembre a diciembre de 2024	El control se encuentra operando correctamente debido a que el proceso responsable remitió todos los soportes correspondientes al cuatrimestre, en el cual de manera semanal se generan los datos y cifras de proyección de personal para la línea 123.	Si
14	Gestión de Emergencias.	3	• Material de capacitación sobre seguridad de la información. • listados de asistencia de las capacitaciones efectuadas entre los meses de septiembre y diciembre de 2024.	De acuerdo a la revisión de las evidencias remitidas por el proceso responsable, el control se está ejecutando correctamente puesto que se están dando capacitaciones en referencia a seguridad de la información y específicamente al manejo de usuarios y contraseñas, esto en relación a los meses de septiembre, octubre, noviembre y diciembre de la vigencia 2024.	Si
15	Gestión de Emergencias.	1	Informes técnicos de las UPS semanales generados desde septiembre a diciembre de 2024.	Se informa que el control se encuentra operando correctamente puesto que el proceso responsable remite los informes técnicos semanales de los ups generados entre los meses de septiembre a diciembre de 2024.	Si
16	Gestión de Emergencias.	1	3 informes de actividades del contrato 760 de 2024.	El proceso responsable remite informe de actividades del contrato 760 (Motorola) correspondientes a los meses de septiembre octubre y noviembre de la vigencia 2024. Dentro de los mencionados informes se describe el cumplimiento de los acuerdos de niveles de servicio y a manera de ejemplo se indica que para el mes de octubre de 2024 se cumplió correctamente este aspecto (ANS). De acuerdo con lo mencionado, el control se encuentra operando correctamente.	Si

Riesgo	Proceso	Control	Evidencia o soporte visualizado	Seguimiento OCI febrero 2025	Cumple
17	Gestión de Emergencias.	1	Pantalla con repositorio de la sala SOARS respecto a PMU.	Se identifican en el repositorio archivos relacionados con la sala SOARS, por tanto el control cuál está operando correctamente, sin embargo y por la cantidad de archivos y la nomenclatura utilizada en el repositorio se recomienda realizar una revisión y ajuste de los archivos que deben permanecer en el repositorio, identificando puntualmente cuáles son las copias de seguridad oficiales de la base de datos de incidentes que establece el control; esta situación se sugiere debe ser realizada por la primera con el acompañamiento de la segunda línea de defensa.	Si
18	Gestión de Emergencias.	1	Pantalla con repositorio de la sala SOARS respecto a PMU.	Como se indicó en el ítem anterior, se identifican en el repositorio archivos relacionados con la sala SOARS, por tanto el control cuál está operando correctamente, sin embargo y por la gran cantidad de archivos y la nomenclatura utilizada en el repositorio se recomienda realizar una revisión y ajuste de los archivos que deben permanecer en el repositorio identificando puntualmente cuáles son las bitácoras de transferencia oficiales que establece el control; de igual manera se sugiere sea revisado por la primera y segunda línea de defensa.	Si
19	Gestión de Seguridad y Convivencia.	1	Un soporte con correo y comentario de accesos otorgados a una funcionaria.	El soporte remitido por la dependencia responsable cumple con lo establecido en el control durante el periodo evaluado, ya que se informa al líder de la dependencia la funcionaria que tiene acceso y edición a las actas de los consejos distritales de seguridad.	Si
20	Gestión de Recursos Físicos al Servicio de la Entidad.	1	• Soportes de la solicitud de remisión de usuarios en el sistema de información • Archivo de usuarios de Progressus con las acciones a realizar.	Se identifica solicitud de usuarios a la DTSI por parte del líder del sistema de información PROGRESSUS, tal como lo referencia el control; adicionalmente se remite archivo con los ajustes que se requieren respecto a los usuarios del sistema de información, correspondientes al mes de diciembre de 2024, con lo informado por el proceso responsable del control, este se encuentra operando correctamente.	Si
20	Gestión de Segurid	2	Un acta de mesa de trabajo sobre	El proceso responsable remite acta de reunión en donde se abordan los ajustes requeridos a la guía para el registro y validación de actividades en el	Si

Riesgo	Proceso	Control	Evidencia o soporte visualizado	Seguimiento OCI febrero 2025	Cumple
	ad y Convivencia.		seguridad de la información.	sistema de información PROGRESSUS de acuerdo a lo estimado en el control, por tanto, este está operando correctamente.	
21	Gestión de Seguridad y Convivencia.	1	Acta seguimiento a cargo de documentación en SharePoint.	El control se está ejecutando correctamente debido a que el proceso responsable remite acta con fecha 27/12/2024, en el cual se hace seguimiento al cargue de la documentación en el Sharepoint de la Dirección de Seguridad, resaltando que en dicha reunión asiste la Directora de Seguridad con la responsable el manejo de la documentación electrónica de la dependencia.	Si
22	Gestión de Seguridad y Convivencia.	1	Cuatro archivos con soportes correspondientes al mes de septiembre, octubre noviembre y diciembre de 2024.	El proceso responsable remite reportes mensuales generados en la plataforma con las actas de los consejos locales de seguridad, informando a todo el personal el estado de estas y solicitando que se debe garantizar la disponibilidad en el sistema de información aprobándolas y validándolas. De acuerdo a lo validado, el control se encuentra operando de manera correcta.	Si
23	Gestión de Seguridad y Convivencia.	1	• Correo en el electrónico solicitando la actualización de registros en formularios. • reporte en Excel de los registros que se deben actualizar.	El control se está ejecutando correctamente ya que vía correo electrónico el responsable del sistema de información solicita a todo el personal la actualización de los registros en el formulario titulado mercados criminales y aspectos sociales como económicos y estructurales. Para este caso se resalta y recomienda que la primera y segunda línea de defensa revisen este control debido a qué si bien se están ejecutando las actividades planteadas, se están presentando errores en los registros que se tienen almacenados en las herramientas de información, por tanto, se están presentando debilidades en cuanto a la integridad de la información.	Si
24	Gestión de Seguridad y Convivencia.	1	• Correo electrónico donde se reporta la correspondencia entre los registros de progresus y survey 123. • Archivo Excel con el	Tal y como se indicó en el caso anterior, el control se está ejecutando correctamente de acuerdo a lo establecido y generando las evidencias requeridas, no obstante, se reitera la recomendación relacionada con la revisión por parte de la primera y segunda línea de defensa de este control puesto que se están presentando falta de correspondencia entre los datos de 2 herramientas derivando en riesgos de integridad	Si

Riesgo	Proceso	Control	Evidencia o soporte visualizado	Seguimiento OCI febrero 2025	Cumple
			reporte de correspondencia entre el sistema de información progresos y survey 123.	de la información, permitiendo concluir que el control no está atacando la causa raíz.	
25	Gestión de Tecnologías de la Información.	1	Archivo Excel con el reporte de service manager correspondiente a la vigencia 2024.	El control no se está ejecutando de acuerdo con lo establecido, puesto que la dependencia responsable remite listado de incidentes de service managers atendido por cada uno de los ingenieros, sin embargo y como el control menciona: "*como evidencia de la ejecución del control se contará con los avances de las actividades del plan mediante bitácoras de actividades, actas y/o comunicado oficial*. ", No se está remitiendo información donde se reporten los avances de las actividades del plan de trabajo de versionamiento de los ambientes de prueba y producción asociados a los sistemas de información de la entidad, razón por la cual, se sugiere a la primera y segunda línea de defensa realizar revisión de este control de manera puntual, para que los soportes que sean generados se ajusten a lo descrito.	No
25	Gestión de Tecnologías de la Información.	2	5 archivos con manuales técnicos de sistemas de información de la entidad.	El proceso responsable remite manuales técnicos de los siguientes sistemas de información: Apelaciones, COPE, SIMBA, Casa libertad, SIRPA y Sitio web. De acuerdo con los soportes remitidos, el control se está cumpliendo parcialmente debido a que no se están asociando los manuales técnicos actualizados de **todos** los sistemas de información de la entidad o el reporte de seguimiento al plan tal y como lo describe el control, por ende, se insta a la primera y segunda línea de defensa a realizar revisión puntual de lo descrito para así generar la completitud de las evidencias que son requeridas.	No
26	Gestión de Tecnologías de la Información.	1	• Documento no controlado sobre la gestión segura de credenciales de administración. • Correo electrónico	El control se está cumpliendo de acuerdo a lo establecido, basado en las evidencias remitidas por la dependencia responsable, sin embargo, se recomienda al proceso responsable oficializar en el sistema integrado de gestión el documento para la gestión segura de contraseñas; adicionalmente y después de tener esto, se insta a la primera y	Si

Riesgo	Proceso	Control	Evidencia o soporte visualizado	Seguimiento OCI febrero 2025	Cumple
			informando al director de la DTSI la creación del documento anterior.	segunda línea de defensa realizar revisión y actualización del control.	
26	Gestión de Tecnologías de la Información.	2	Documento técnico titulado PERFORMANCE.	El proceso responsable remite en el documento técnico el reporte de rendimiento de la infraestructura de seguridad de la entidad. De acuerdo a lo informado, el control se encuentra operando correctamente.	Si
27	Gestión Estratégica del Talento Humano.	1	3 soportes de correo electrónico solicitando permisos en el sistema SIAP.	El control está operando correctamente puesto que la dependencia responsable remite evidencias asociadas a la aprobación de permisos sobre el sistema de nómina SIAP. Desde la OCI se informa a la segunda línea de defensa acerca de la revisión de los soportes documentales en el repositorio oficial para riesgos de seguridad de la información, puesto que los riesgos de talento humano se encuentran titulados y/o codificados con los números 9 y 10.	SI
28	Gestión Estratégica del Talento Humano.	1	4 evidencias de consulta y préstamo de expedientes laborales correspondientes a los meses de octubre noviembre y diciembre de 2024.	El proceso responsable remite las bitácoras (planillas) donde se registran las consultas y préstamos de historias laborales al personal de la entidad, suscitadas en los meses de octubre, noviembre y diciembre de la vigencia 2024, con lo anterior, se concluye que el control se está ejecutando correctamente.	Si
29	Gestión Financiera.	1	3 evidencias de correos electrónicos tramitados al interior de la dependencia responsable	El control se encuentra operando correctamente, debido a que la dependencia responsable remite correos electrónicos informando puntualmente que, para el último cuatrimestre de la vigencia, no se tramitaron solicitudes de accesos a los sistemas de información; para este caso, se recomienda principalmente a la primera línea de defensa monitorear y ejecutar el control cuando se presente un caso donde se requiera acceso de usuarios nuevos al sistema de información bajo su responsabilidad.	Si

Riesgo	Proceso	Control	Evidencia o soporte visualizado	Seguimiento OCI febrero 2025	Cumple
30	Gestión Integral a las Personas Privadas de la Libertad - PPL.	1	Correo electrónico reportando la ejecución del control.	Una vez revisado el soporte remitido por el proceso responsable, se indica que el control está operando correctamente ya que se genera correo electrónico con fecha 07/01/2025 dirigido al Director del Centro Especial de Reclusión, informando las solicitudes de acceso a la información de historias de vida de PPL y donde se validó que estas estuvieran aprobados y autorizadas por la Dirección, adicionalmente se reporta dentro del mismo correo electrónico la ejecución del control relacionado con las llaves del archivador de la documentación física que se encuentra ubicado dentro del área administrativa del centro.	Si
31	Gestión Jurídica.	1	Formato FUID de la vigencia 2024.	La dependencia responsable remite inventario documental de la vigencia 2024, con lo cual se cumple lo establecido en el control.	Si
32	Gestión Tecnológica de Seguridad y Emergencias.	1	• 4 informes mensuales Correspondientes a los meses de septiembre y octubre • 3 actas de conciliación correspondientes a los meses de septiembre y octubre.	Si bien el control se encuentra operando correctamente, se informa la incompletitud de las evidencias, ya que solamente se adjuntan los correspondientes a los meses de septiembre y octubre, haciendo énfasis en que el control indica que se debe presentar el reporte mensual de los mantenimientos realizados y avalados por la interventoría y/o supervisión, es decir que queda pendiente aportar evidencias del mes de noviembre.	Si
32	Gestión Tecnológica de Seguridad y Emergencias.	2	4 documentos relacionados con los informes mensuales correspondientes a los meses de septiembre y octubre.	Cómo se indicó en el control anterior, este está operando correctamente, sin embargo, el proceso responsable no está adjuntando los soportes generados para los meses de noviembre y diciembre, por tal motivo, se recomienda la primera y segunda línea de defensa realizar monitoreo de los soportes que se deben generar en cada corte establecido de acuerdo con la política de administración de riesgos de la entidad.	Si
33	Gestión y Análisis de la Información.	1	2 reportes de consulta la bodega de datos correspondiente a los meses de septiembre y octubre de 2024.	El proceso responsable remite como soporte las consultas SQL Ejecutadas y el formato con código 581, donde se lleva registro de cargas de información a la bodega de datos por parte de la Oficina de Análisis de la Información y Estudios Estratégicos.	No

Riesgo	Proceso	Control	Evidencia o soporte visualizado	Seguimiento OCI febrero 2025	Cumple
			4 formatos F-GI-581 correspondiente a los meses de septiembre, octubre, noviembre y diciembre	La OCI informa que el control se está ejecutando parcialmente, puesto que dentro de su texto se indica que " *Como evidencias se adjunta la consulta SQL y el cargue en el portal MIPG del indicador de gestión asociado.* ", informando que dentro de los soportes no se evidencia el cargue en el portal MIPG el indicador de gestión asociado, por tanto, se recomienda a la primera y segunda línea de defensa realizar revisión de lo descrito por el control y generando los soportes asociados tal y como se describe para cada corte de seguimiento.	

Tabla N° 4: - Elaboración propia – Fuente: repositorio evidencias ejecución de controles asociados a riesgos de seguridad de la información administrada por la DTSI.

5. CONCLUSIONES DE AUDITORÍA

En este acápite, se presentan las conclusiones derivadas del ejercicio de seguimiento y evaluación al tema de riesgos de seguridad de la información. El objetivo principal de este análisis como se indicó en la parte introductoria ha sido revisar y valorar la gestión de los controles a través de las medidas implementadas para gestionar los riesgos mencionados, todo esto con el fin de buscar y/o fortalecer la protección de los activos de información de la Secretaría. A continuación, se referencian los temas considerados relevantes por la OCI:

- **Adición de riesgos y controles para procesos dentro de la matriz de riesgos de seguridad de la información después de una materialización**: En la vigencia 2024 se presentó una materialización de riesgo relacionado con documentación física y que involucra a los procesos de Fortalecimiento y Acceso a la Justicia y al proceso de Gestión Documental, este ultimo y debido a lo sucedido no ha incluido / sugerido de manera oficial riesgos y controles dentro de la matriz de riesgos de seguridad de la información, para dar el tratamiento acorde y basado en la importancia que implica para la entidad un evento donde se presente deterioro, daño o eliminación documental de manera no controlada.

- **Integridad de datos en la matriz de riesgos de seguridad de la información**: De acuerdo con los temas de integridad (codificaciones, cantidades de activos de información de los procesos, entre otros aspectos). La matriz de riesgos de seguridad de la información presenta situaciones con la

calidad de la información que deben ser abordadas principalmente por la segunda línea de defensa al momento de ejecutar sus validaciones y monitoreos.

- **Actualización de riesgos y controles**: Como se pudo evidenciar al final de la vigencia 2024 y derivado de las actualizaciones que realizaron a 5 procesos de la entidad, se confirma que los riesgos y controles de seguridad de la información es un tema dinámico que requiere continua validación y adaptación, por tanto, la ejecución de ejercicios de acompañamiento periódico permitirá a la totalidad de los procesos actualizar y ajustar a la realidad operativa, identificando nuevas amenazas y vulnerabilidades.

- **Fortalecimiento en la generación de evidencias a reportar por cada corte:** Una vez efectuado el ejercicio auditor, se concluye que las dependencias responsables de la ejecución de los procesos han fortalecido la generación y reporte de evidencias y/o soportes, no obstante, aún se presentan debilidades, principalmente en lo que describe detalladamente el control versus los soportes que dan fe de su cumplimiento.

- **Fortalecimiento de la calificación del control:** Los controles actualmente se evalúan y califican de acuerdo a lo establecido en la Política de Administración del Riesgo, sin embargo para fortalecer este aspecto, es importante sea revisado de manera integral todas las variables que indican tanto los documentos internos del SIG como lo indicado por las buenas prácticas de la industria en materia de riesgos, buscando el aumento en la efectividad y eficiencia de los controles, mencionando a manera de ejemplo la inclusión de variables tales como la automatización o manualidad de estos, lo cual opera como insumo para establecer nuevas estrategias.

6. RECOMENDACIONES

- Revisar y actualizar la política de administración de riesgos en su capítulo de seguridad de la información y/o digital, así como también la matriz de riesgos de seguridad de la información.

- Realizar un análisis costo beneficio aprovechando las herramientas con las cuales cuenta actualmente la entidad para automatizar la matriz de riesgos de seguridad de la información, incluyendo aspectos que permitan el mejoramiento continúo debido a la dinámica del tema. Entre otros aspectos, se sugiere validar aspectos como el registro de la información por parte de las diferentes líneas de defensa, con el fin de fortalecer el seguimiento y con esto establecer acciones de mejora al momento de identificar desviaciones o debilidades, así como también permite de manera mas efectiva realizar procesos de actualización o ajustes tanto de riesgos como de controles.

- Intensificar por parte de la segunda línea de defensa el monitoreo y revisión periódica respecto a lo establecido en los controles, así como también en la generación de evidencias, las cuales deben ser concordantes y coherentes tal como se conceptuaron.

- Incluir de manera inmediata nuevos riesgos y controles al momento de presentarse materialización de riesgos, adicionalmente incrementar los procesos de comunicación y socialización a toda la entidad, para que se tenga la claridad para identificar y reportar los eventos relacionados con la afectación de la información tanto física como electrónica.

Elaboró:

Diego Alexander Urazán Franco

Contratista Oficina de Control Interno

Aprobó:

Karol Andrea Parraga Hache

Jefe Oficina de Control Interno