ALCALDÍA MAYOR DE BOGOTÁ
SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA
AL RESPONDER CITAR EL NR.
Nro. Rad: 3-2025-24957
Fecha: 27/06/2025 07:42:35 PM
Destino: 100-DESPACHO

MEMORANDO

Para: CESAR ANDRES RESTREPO FLOREZ
DESPACHO SECRETARIO DE SEGURIDAD

De: OFICINA DE CONTROL INTERNO

Asunto: INFORME DE SEGUIMIENTO A LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN I CUATRIMESTRE DE 2025

Cordial saludo, Dr. Restrepo Florez:

En cumplimiento de lo estipulado en el Artículo 17 del Decreto 648 de 2017, relativo al rol de "*Evaluación de la Gestión del Riesgo*" definido por el Departamento Administrativo de la Función Pública, así como en atención a la ejecución del Plan Anual de Auditoría de la 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 presenta el Informe de Seguimiento a los Controles asociados a los Riesgos de Seguridad de la Información, correspondiente al primer cuatrimestre de 2025, en el cual, de manera general, se concluye lo siguiente:

- Se evidencian avances en la identificación, implementación, monitoreo y seguimiento asociados a los riesgos de seguridad de la información, destacándose la articulación entre las líneas de defensa y el cumplimiento de la política institucional.

- Persisten oportunidades de mejora detectadas en el Informe de Seguimiento a los Riesgos de seguridad de la Información tercer cuatrimestre 2025, Radicado N. 3-2025-7706.

- Por otra parte, se Identificó la falta de inclusión del proceso de Gestión de Conocimiento e Innovación Pública en los registros de activos en concordancia con las tablas de retención documental, así como en atención a la Guía de Administración del Riesgo de la SDSCJ (G-FI-04 V3).

- También, se observó que actualmente la valoración de riesgos de seguridad de la información se basa en vulnerabilidades identificadas en lugar de amenazas, lo cual requiere validación y ajuste, toda vez que los resultados no son consistentes con el número de riesgos determinados por proceso y desatienden lo estipulado en el numeral 6.3 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6, emitida por el DAFP.

- Se identificaron brechas en la documentación y trazabilidad de algunas actividades de control, especialmente aquellas relacionadas con la respuesta ante desviaciones, así como debilidades en la evidencia de ejecución de controles.

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: 3-2025-24957
Fecha: 27/06/2025 07:42:35 PM
Destino: 100-DESPACHO

De otro lado, a partir de los resultados del seguimiento realizado, se deberá formular el Plan de mejoramiento al que haya lugar, en el aplicativo ITS-Portal MIPG, de acuerdo con lo establecido en el Procedimiento “Plan de Mejoramiento Interno PD-SM-4”. El tiempo máximo para la formulación y registro del plan de mejoramiento interno será de ocho (8) días hábiles, contados a partir de la comunicación y/o notificación que generará el aplicativo mencionado. La Oficina de Control Interno realizará la verificación de las acciones propuestas en términos de eficiencia y eficacia.

Finalmente, es preciso informar que, el informe adjunto será publicado en la sección de transparencia de la Secretaría de Seguridad, Convivencia y Justicia en la siguiente ruta: https://scj.gov.co/es/transparencia/planeacion-presupuesto-ingresos/informes-control-interno.

Cordialmente,

KAROL ANDREA PARRAGA HACHE
JEFE DE OFICINA CONTROL INTERNO

c.c.e.: JAIRO ALONSO BOHORQUEZ BLANCO-DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION
JULIAN PONTON SILVA-OFICINA ASESORA DE PLANEACION
Anexos: -1

Elaboró: INGRID BEATRIZ ACOSTA VELASQUEZ
Revisó: KAROL ANDREA PARRAGA HACHE-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 LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN PRIMER CUATRIMESTRE 2025

2025

Oficina de Control Interno

ALCALDÍA MAYOR DE BOGOTÁ D.C.

SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA

BOGOTÁ

Tabla de contenido

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 - SDSCJ, de acuerdo con la Política de administración de Riesgos PO-FI-02 V2 y la Guía de Administración de Riesgos G-FI-04 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 y la Guía de Administración de Riesgos G-FI-04 V3.
- Verificar si los procesos de la SDSCJ cuentan con riesgos y 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 observaciones y 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 enero al 30 de abril de 2025, 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 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 AUDITORIA

- 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 AUDITORIA

4.1 CUMPLIMIENTO POLÍTICA ADMINISTRACIÓN DE RIESGOS.

La Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ, dispone de documentos internos que establecen los lineamientos esenciales para la gestión de riesgos de seguridad de la información asociados a los activos de información identificados en los distintos procesos de la entidad. Entre estos documentos, se destacan la Política de Administración de Riesgos y la Guía de Administración de Riesgos, esta última con especial énfasis en el acápite N.º 11, titulado “Identificación y Gestión del Riesgo (Riesgo Seguridad de la Información)”. Dichos lineamientos permiten identificar amenazas, vulnerabilidades, impactos, niveles de riesgo, valoraciones y tratamientos adecuados, mediante una metodología estructurada que define etapas clave para su implementación efectiva. Lo anterior permite una gestión de riesgos oportuna, eficiente y alineada con los objetivos estratégicos institucionales, promueve una cultura organizacional en torno a la seguridad de la información y posibilita una toma de decisiones fundamentada en el análisis de riesgos.

En este contexto, y conforme al alcance del presente informe, a continuación, se detalla la gestión realizada por la Secretaría en cada una de las etapas definidas:

4.1.1 ETAPA 1: CONOCIMIENTO Y DIVULGACIÓN:

Se observó que, el 25 de abril de 2025, la Dirección de Tecnologías y Sistemas de la Información (DTSI) llevó a cabo la difusión, a través de correo electrónico, de una pieza gráfica titulada “*Seguimiento de Control de Riesgos de Seguridad de la Información”*. Esta comunicación fue enviada de manera masiva a toda la Entidad como parte de sus actividades de socialización, como se ilustra:

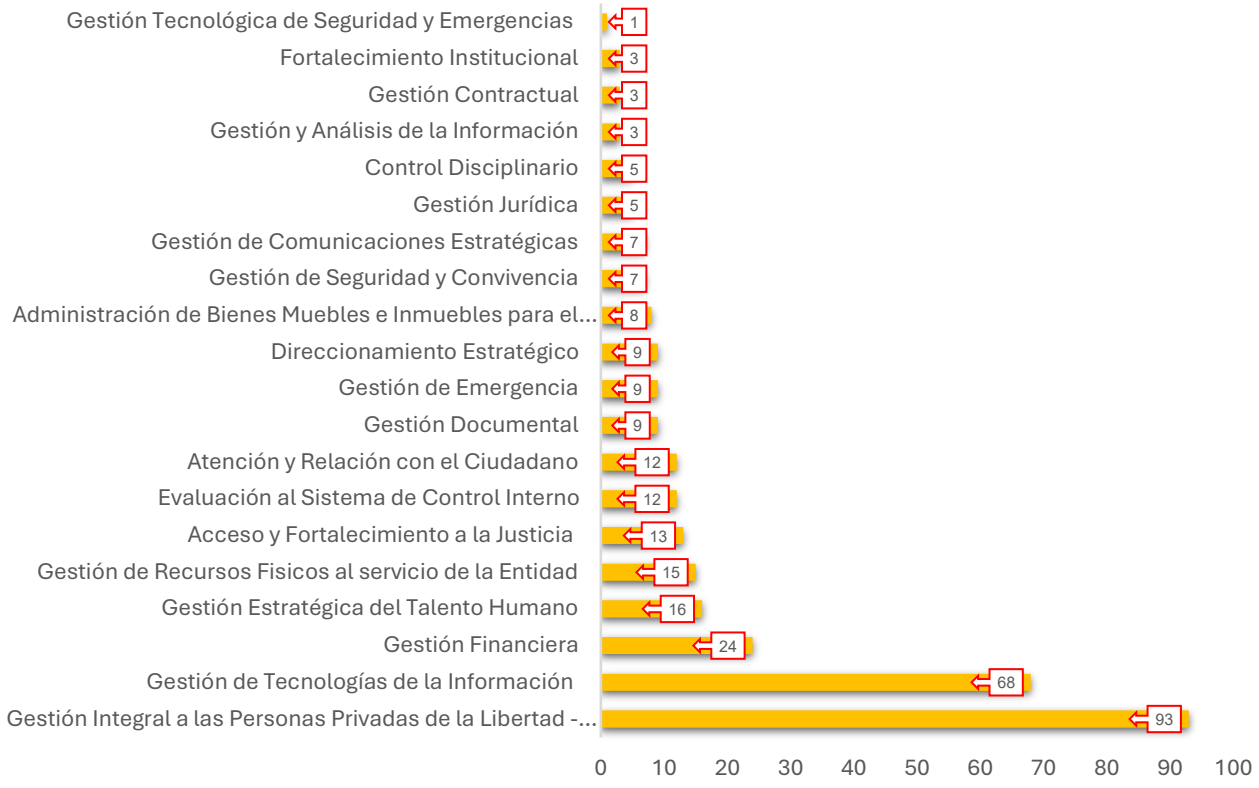
Imagen N°1: Pieza comunicacional remitida por la DTSI a toda la entidad vía correo electrónico el día 25/04/2025. Fuente: INFORME PRIMER CUATRIMESTRE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN - 2025 generado por la DTSI con radicado número 3-2025-13744

Se verificó que la Dirección de Tecnologías y Sistemas de la Información (DTSI) emitió el memorando electrónico digital 3-2025-13744, el 8 de abril de 2025, instruyendo a los procesos responsables sobre el cargue de evidencias relacionadas con los controles implementados para mitigar los riesgos de seguridad de la información, correspondientes al primer cuatrimestre de la vigencia 2025. Asimismo, se constató que dicha información también fue difundida, mediante correo electrónico, el 28 de abril de 2025 a todas las áreas responsables de la gestión de riesgos de seguridad de la información. El mensaje incluyó orientaciones específicas sobre el procedimiento para el cargue de evidencias del primer cuatrimestre, y la solicitud de validación de las observaciones formuladas por la Oficina de Control Interno respecto a los informes emitidos sobre los riesgos de seguridad de la información durante la vigencia 2024.

4.1.2 ETAPA 2: IDENTIFICACIÓN DE ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN:

De acuerdo con el informe radicado 3-2025-19176 de la DTSI, correspondiente al primer cuatrimestre de 2025 sobre riesgos de seguridad de la información, y tras la verificación de la información adicional entregada, se determinó que la entidad posee un total de 322 activos de información asociados a sus procesos. En consecuencia, se ha venido actualizando tanto el registro de activos de información como el índice de información clasificada y reservada, siendo este publicado, en cumplimiento de la Ley de Transparencia en el siguiente vínculo: *Registros de Activos de Información | Secretaría Distrital de Seguridad, Convivencia y Justicia*.

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



Gráfica 1. Cantidad de activos de Información por proceso. Elaboración Oficina de Control Interno, Fuente: Matriz de riesgos de seguridad de la información F-FI-1385 - I Cuatrimestre 2025

Se efectúo la revisión de la información reportada en el Informe radicado N. 3-2025-19176, y se constató, mediante el reporte de actas, la realización de las mesas de trabajo efectuadas en el periodo evaluado (enero - abril de 2025), entre la Dirección de Recursos Físicos y Gestión Documental, en coordinación con la Dirección de Tecnologías y Sistemas de la Información y el proceso de Gestión de Emergencias, en donde se revisaron los activos de información, en atención a la incorporación de nuevos activos asociados a dicho proceso.

Asimismo, se evidenció el acta correspondiente a la mesa de trabajo con el proceso de Gestión Documental, orientada a la actualización del borrador del formato F-GD-1081 – Registro de Activos de Información e Índice de Información Clasificada y Reservada, con miras a su trámite y aprobación ante la Oficina Asesora de Planeación, y su posterior publicación en el Portal MIPG de la Entidad.

Por otra parte, se observa que, el Registro de Activos de Información y el Índice de Información Clasificada y Reservada, actualmente disponible en el sitio web institucional, corresponde a la publicación realizada el día 29 de noviembre de 2024, accesible en el siguiente enlace: *Registros de Activos de Información | Secretaría Distrital de Seguridad, Convivencia y Justicia*. Y dado que no se ha publicado una nueva versión de actualización para el primer cuatrimestre de 2025, la matriz de activos de información vigente no refleja los ajustes y/o modificaciones realizadas en dicho período de evaluación, por ello, se determina la siguiente oportunidad de mejora:

OPORTUNIDAD DE MEJORA 1.

La falta de publicación, en la página web de la SDSCJ, de una versión actualizada de la matriz de activos de información correspondiente al primer cuatrimestre de 2025, no permite tener una validación actual de los ajustes y modificaciones realizados durante dicho periodo. Esto limita la visibilidad de los avances logrados y compromete la trazabilidad de la información. Por tanto, se recomienda emitir una nueva versión que refleje, de forma precisa y documentada, el progreso alcanzado con los diferentes procesos.

4.1.3 ETAPA 3: PASOS PARA LA IDENTIFICACIÓN Y/O VALORACIÓN DE ACTIVOS:

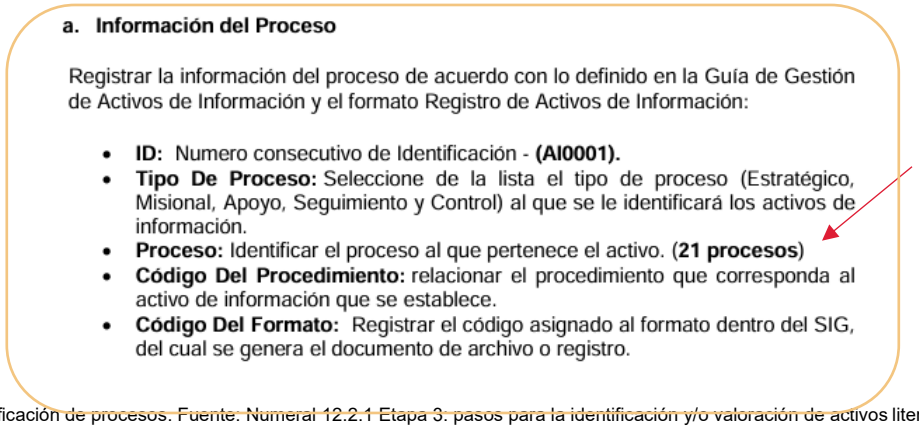
Se constató que, tanto en el registro de activos de información F-GD-1081, como en la Matriz de Riesgos de Seguridad de la Información - 2025 F- FI-1385, se incluyen los ocho (8) criterios definidos en la guía de administración de riesgos G-FI-04 V.3:

Imagen 2. Criterios para identificación de riesgos. Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC

Asimismo, se verificó que la criticidad de los activos de la Secretaría Distrital de Seguridad, Convivencia y Justicia, está clasificada de acuerdo con el grado de importancia de cada Activo de información, conforme a los criterios de Confidencialidad, Integridad y Disponibilidad (Alta, Media Baja), lo cual permite, posteriormente, realizar el análisis de riesgos y establecer una valoración adecuada en cada caso, con base al resultado obtenido.

Al analizar los registros de activos de información F-GD-1081 por procesos, se identificó que el proceso de Gestión de Conocimiento e Innovación Pública no está incluido en dicho documento, lo cual resulta inconsistente con lo establecido en el numeral 12.2.1, Etapa 3: Pasos para la identificación y/o valoración de activos, literal a, de la Guía de Administración de Riesgos G-FI-

04 V.3. Este numeral enfatiza la inclusión de los 21 procesos sin excepciones, y no justifica la omisión de ninguno. Actualmente, el reporte de activos contempla 20 procesos, como se ilustra:



a. Información del Proceso

Registrar la información del proceso de acuerdo con lo definido en la Guía de Gestión de Activos de Información y el formato Registro de Activos de Información:

- **ID:** Numero consecutivo de Identificación - **(AI0001).**
- **Tipo De Proceso:** Seleccione de la lista el tipo de proceso (Estratégico, Misional, Apoyo, Seguimiento y Control) al que se le identificará los activos de información.
- **Proceso:** Identificar el proceso al que pertenece el activo. (**21 procesos**)
- **Código Del Procedimiento:** relacionar el procedimiento que corresponda al activo de información que se establece.
- **Código Del Formato:** Registrar el código asignado al formato dentro del SIG, del cual se genera el documento de archivo o registro.

Imagen N. 3. Identificación de procesos. Fuente: Numeral 12.2.1 Etapa 3. pasos para la identificación y/o valoración de activos literal a. de la Guía de Administración de Riesgos G-FI-04 V.3

Adicionalmente, en la Secretaría Distrital de Seguridad, Convivencia y Justicia - SDSCJ, en los riesgos de seguridad de la información, se identifican (tipo de amenazas, vulnerabilidades, Impacto, niveles de riesgos, y tratamientos) con base en los activos de información alineado a las **Tablas de Retención Documental**, cumpliendo con los lineamientos para la gestión de riesgos en Seguridad digital en las Entidades públicas, de acuerdo a lo establecido en el Modelo de Seguridad y Privacidad de la Información (MSPI), del Ministerio de Tecnologías de la Información – MINTIC. Por lo sustentado en el presente acápite, se presenta la siguiente oportunidad de mejora.

OBSERVACION 1: FALTA DE INCLUSIÓN DEL PROCESO DE GESTIÓN DEL CONOCIMIENTO EN EL REGISTRO DE ACTIVOS DE INFORMACIÓN.

Se evidenció por parte de equipo auditor que el proceso de *Gestión de Conocimiento e Innovación Pública* no fue incluido en los registros de activos de información (formato F-GD-1081), lo cual incumple lo dispuesto en la Guía de Administración de Riesgos G-FI-04 V.3, que establece la obligatoriedad de considerar los 21 procesos institucionales sin excepción. Esta omisión genera una falta de alineación con las tablas de retención documental y debilita la gestión integral de riesgos de seguridad de la información, al dificultar la identificación y tratamiento de amenazas y vulnerabilidades asociadas al proceso no registrado.

Recomendación: Incluir los activos de información correspondientes al proceso *Gestión de Conocimiento e Innovación Pública* en el formato F-GD-1081, garantizando su alineación con las directrices de la Guía G-FI-04 V.3 y fortaleciendo la gestión documental y de riesgos de seguridad de la información.

4.1.4 ETAPA 4: IDENTIFICACIÓN DEL RIESGO:

Como se mencionó, en el análisis de la matriz de riesgos de seguridad de la información de la entidad (F-FI-1385), se identifican 322 activos clasificados según su criticidad: alta (71), moderada (154) y baja (97), dentro de una estructura organizada, donde cada riesgo cuenta con amenazas, vulnerabilidades y consecuencias definidas, así como con la determinación de su probabilidad, impacto y niveles de riesgo inherente y residual.

Además, cada riesgo tiene controles asociados para su mitigación, con una distribución específica por cada proceso, como se detalla:

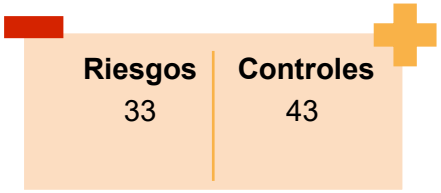
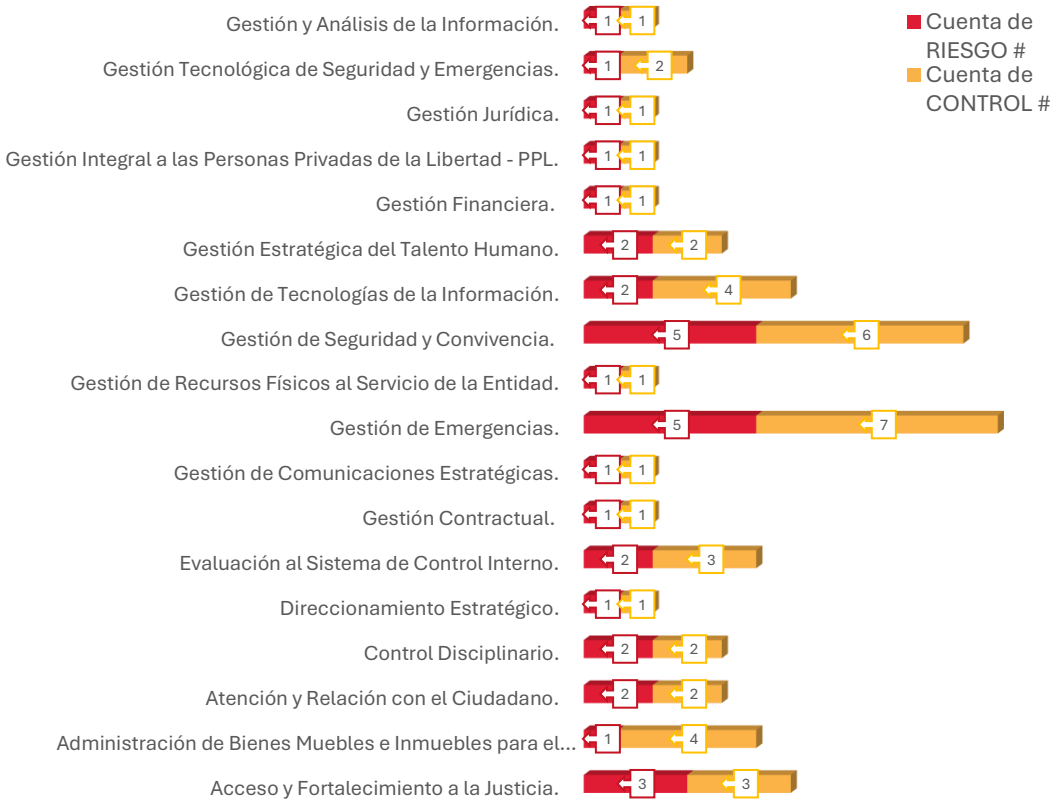


Imagen N. 4 Riesgos y Controles asociados, Fuente: Matriz de riesgos de seguridad de la información F-FI-1385 - I Cuatrimestre 2025



Gráfica N. 2 Cantidad de Riesgos y controles de Seguridad de la Información por proceso. Elaboración Oficina de Control Interno. Fuente: Matriz de riesgos de seguridad de la información F-FI-1385 - I Cuatrimestre 2025

Por otra parte, se identificó que la matriz de riesgos cumple con los criterios mínimos establecidos para su identificación; sin embargo, en el marco de la mejora continua, se recomienda tener en cuenta lo dispuesto en el CONPES 3995 de 2020, "*Política Nacional de Confianza y Seguridad Digital",* que promueve la preparación ante incidentes cibernéticos, incluyendo la elaboración de planes de respuesta ante tales eventos. Asimismo, se sugiere considerar lo establecido por la norma técnica NTC-ISO/IEC 27001:2022, la cual define los requisitos para sistemas de gestión de seguridad de la información, entre ellos la identificación, monitoreo y revisión de riesgos. Igualmente, se destaca la importancia de definir indicadores de riesgo para su monitoreo continuo y establecer mecanismos de revisión y actualización periódica de la matriz, garantizando así su adaptación frente a nuevos escenarios y transformaciones tecnológicas. Finalmente, se recomienda contemplar lo estipulado en el Decreto 612 de 2018, que exige a las entidades distritales incorporar planes de tratamiento de riesgos de seguridad y privacidad de la información dentro del Modelo Integrado de Planeación y Gestión (MIPG).

En análisis de la Matriz de Riesgos de Seguridad de la Información de la Entidad (F-FI-1385), se identificó que en la pestaña "Tratamiento de los riesgos", las causas mitigadas corresponden a las vulnerabilidades documentadas en la pestaña "Riesgo Inherente", cumpliendo lo que establece la guía, frente a que las vulnerabilidades son funcionales para el análisis de las causas:

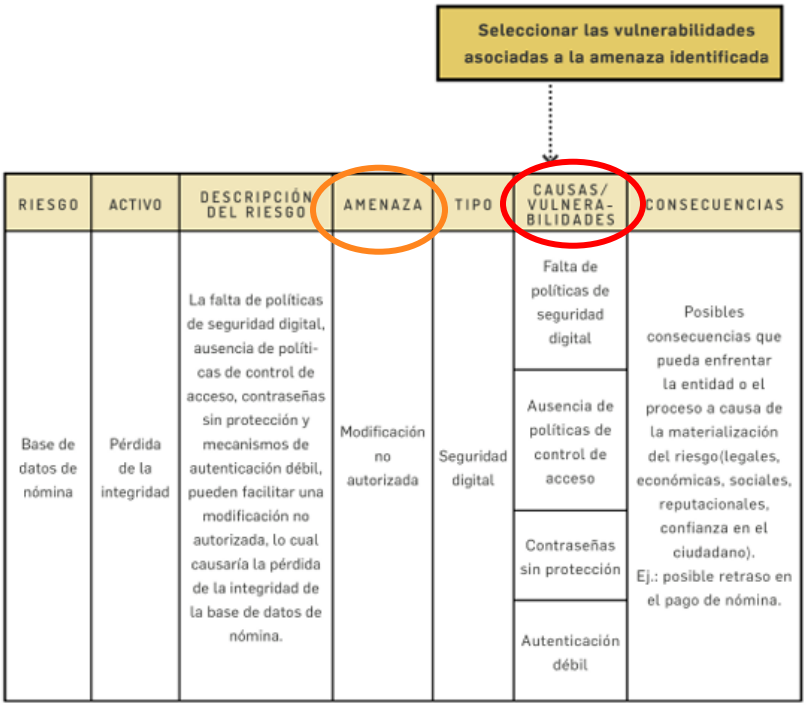


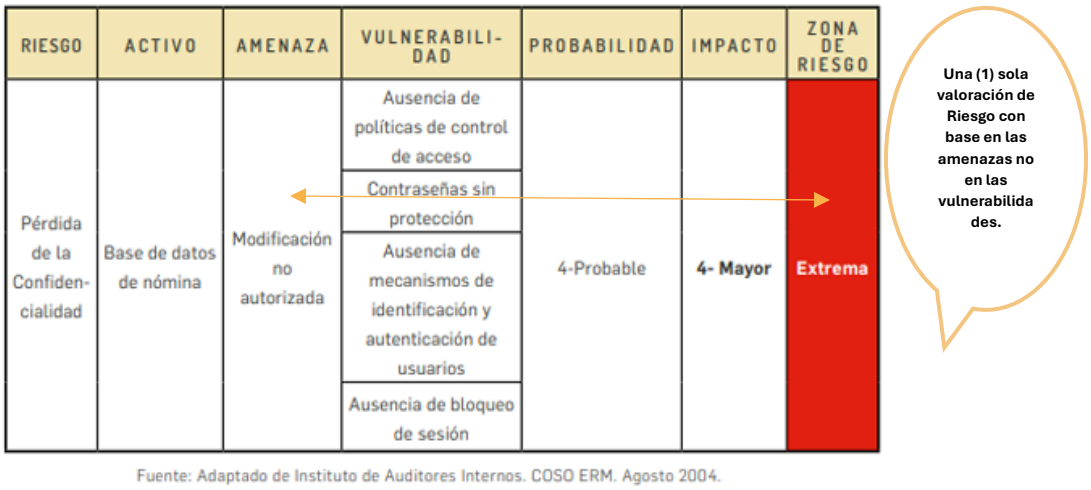
Imagen N. 5. Fuente: Numeral 6.2 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6.

A continuación, se observa un ejemplo (Riesgo N.4), las causas que relacionan son las mismas vulnerabilidades identificadas, siendo coherente con la anterior ilustración:

TRATAMIENTO DE RIESGO						RIESGO INHERENTE	
RIESGO #	PROCESO	CONTROL #	TIPO DE ACCIÓN	CAUSA MITIGADA	CONSECUENCIA MITIGADAS	AMENAZA	VULNERABILIDAD
4	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	1	Reducir el riesgo	Falla en la producción de informes de gestión.	Interrupción de los sistemas / procesos	Error en el uso	Falla en la producción de informes de gestión.
4	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	2	Reducir el riesgo	Gestión deficiente de las contraseñas.	Interrupción de los sistemas / procesos	Error en el uso	Gestión deficiente de las contraseñas.
4	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	3	Reducir el riesgo	Uso incorrecto de software y hardware.	Interrupción de los sistemas / procesos	Error en el uso	Uso incorrecto de software y hardware.
4	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	4	Reducir el riesgo	Rotación de Personal	Interrupción de los sistemas / procesos	Error en el uso	Rotación de Personal

Tabla N. 1. Vulnerabilidades para análisis de causas. Elaboración OCI. Fuente. Matriz de riesgos de seguridad de la información F-FI-1385 - I Cuatrimestre 2025

No obstante, se observó que en la matriz de riesgos (F-FI-1385) no se está considerando la valoración del riesgo inherente con base en las amenazas, sino en las vulnerabilidades, lo que difiere de lo señalado en la Guía para la administración de los riesgos del DAFP V6, como se ilustra a continuación:



Fuente: Adaptado de Instituto de Auditores Internos. COSO ERM. Agosto 2004.

Imagen. 6. Fuente: Numeral 6.3 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6.

Complementariamente, se presenta el siguiente ejemplo (Riesgo N. 4), que muestra la valoración de riesgo inconsistente (un único riesgo con 4 valoraciones, con base en las vulnerabilidades y no en las amenazas):

RIESGO #	PROCESO	RIESGO	AMENAZA	VULNERABILIDAD	PROBABILIDAD	IMPACTO	RIESGO INHERENTE
4	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	Pérdida de la Integridad	Error en el uso	Falla en la producción de informes de gestión.	Media	Leve	MODERADO
4	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	Pérdida de la Integridad	Error en el uso	Gestión deficiente de las contraseñas.	Media	Leve	MODERADO
4	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	Pérdida de la Integridad	Error en el uso	Uso incorrecto de software y hardware.	Media	Leve	MODERADO
4	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	Pérdida de la Integridad	Error en el uso	Rotación de Personal	Baja	Moderado	MODERADO

Tabla N. 2 Valoración de Riesgo con base en vulnerabilidades. Elaboración Oficina de Control Interno; Fuente: Matriz de riesgos de seguridad de la información F-FI-1385 - I Cuatrimestre 2025

De lo anterior, se observó que se requiere atender lo estipulado en el numeral 6.3 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6, emitida por el DAFP, que señala:

Imagen N. 7. Fuente: Numeral 6.3 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6.

Es preciso tener en cuenta que un riesgo de seguridad de la información es una amenaza específica que afecta la confidencialidad, integridad o disponibilidad de los activos de información. En su análisis, se identifican riesgos inherentes, que representan la exposición inicial sin considerar controles de mitigación, aunque cada riesgo de seguridad puede tener múltiples factores de riesgo, como las vulnerabilidades, es necesario determinar un único nivel de riesgo inherente basado en su impacto y probabilidad con base en las amenazas por cada riesgo identificado.

OBSERVACION N. 2 INCONSISTENCIAS EN LA VALORACIÓN DE LA PROBABILIDAD O IMPACTO CON BASE EN LAS VULNERABILIDADES.

Se evidenció que la entidad está evaluando la probabilidad e impacto de los riesgos con base en las **vulnerabilidades no frente a las amenazas**, incumpliendo lo establecido en el numeral 6.3 de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas Versión 6 del DAFP, estas situaciones pueden conllevar a un inadecuado tratamiento y administración de los riesgos de seguridad de la información y posible materialización de estos.

Recomendación: Adelantar las acciones pertinentes en el marco del cumplimiento de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas Versión 6 del DAFP.

Por otra parte, en seguimiento de la gestión realizada con base en las observaciones y recomendaciones emitidas por la Oficina de Control Interno a través del Informe de Seguimiento a los Riesgos de seguridad de la Información tercer cuatrimestre 2025, Radicado N. 3-2025-7706 en la etapa de identificación de los riesgos, se obtuvo el siguiente resultado:

OPORTUNIDAD DE MEJORA	REPORTE DE LA SEGUNDA LÍNEA DE DEFENSA (DTI)	SEGUIMIENTO TERCERA LÍNEA DE DEFENSA (OFICINA DE CONTROL INTERNO)
Oportunidad de Mejora N°1: 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.	Se adelantó mesa de trabajo con el personal de la Dirección de Recursos Físicos y Gestión Documental (DRFGD), Durante la sesión se establecieron diversas consideraciones, destacándose como prioridad la necesidad de robustecer los controles establecidos para la gestión de riesgos por proceso. Asimismo, se enfatizó la importancia de crear y formalizar riesgos y controles específicos asociados a la seguridad de la información. En este sentido, se programarán para el segundo	**Resultado:** Aunque el proceso indica que se llevó a cabo una mesa de trabajo donde se establecieron diversas consideraciones para el proceso de Recursos Físicos, aún no se ha realizado la identificación, análisis y documentación de los riesgos correspondientes. Se reporta que esta actividad se programará para el segundo trimestre de 2025.

OPORTUNIDAD DE MEJORA	REPORTE DE LA SEGUNDA LÍNEA DE DEFENSA (DTI)	SEGUIMIENTO TERCERA LÍNEA DE DEFENSA (OFICINA DE CONTROL INTERNO)
	cuatrimestre de la vigencia 2025, las mesas de trabajo orientadas a: • La actualización y categorización de los activos de información de la DRFGD. • La identificación, análisis y documentación de los riesgos de seguridad de la información correspondientes.	Por lo anterior, **se reitera la Oportunidad de Mejora N°1** **Recomendación:** Priorizar la identificación, análisis y documentación de los riesgos antes del segundo trimestre de 2025. Esto permitirá anticipar posibles inconvenientes, optimizar la toma de decisiones y garantizar una planificación eficiente. Además, se sugiere establecer mecanismos de seguimiento para asegurar el cumplimiento oportuno de esta actividad.
Oportunidad de Mejora N°2: 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 informa que ya se realizaron los ajustes correspondientes. Se llevó a cabo una revisión y actualización de los activos de información vinculados al proceso "Acceso y Fortalecimiento a la Justicia", garantizando la consistencia entre la hoja “Listado De Activos” y la hoja “Riesgo Inherente” de la matriz. Actualmente, ambos listados presentan concordancia en cuanto a los ítems y descripciones, en cumplimiento con la metodología institucional. Adicionalmente, se realizó la incorporación de las amenazas identificadas en la matriz F-FI-1385 que no estaban previamente catalogadas en el borrador de la actualización de la G-FI-04: Guía de Administración del Riesgos presentada a la Oficina Asesora de Planeación para la actualización documental en el Portal MIPG.	**Resultado:** Se observa la ejecución de la acción de mejora con la validación de la concordancia en cuanto a ítems y descripciones de los activos de información dentro Formato F-GD-1081 Registro de Activos de Información y la Matriz de Riesgos de Seguridad de la Información. Por lo anterior, **Se subsana la oportunidad de mejora N. 2**
Oportunidad de Mejora N°3: 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	Durante el proceso de revisión, se identificó una serie de amenazas relacionadas con la seguridad de la información que no estaban previamente contempladas en la guía institucional para la administración de riesgos (G-FI-04). Se realizó la incorporación de las amenazas identificadas en la matriz F-FI-1385 que no estaban previamente catalogadas en el borrador de la actualización de la G-FI-04: Guía de Administración del Riesgos presentada a la Oficina Asesora de Planeación para la actualización documental en el Portal MIPG.	**Resultado:** Se observa la actualización de los siguientes documentos: PO-FI-02: Política de Administración de Riesgos. • G-FI-04: Guía de Administración del Riesgos. • F-FI-1385: Matriz de Riesgos de Seguridad de la Información. Por lo anterior, **Se subsana la oportunidad de mejora N. 3**

Tabla N. 3. Gestión Adelantada frente a las Oportunidades de Mejora emitidas por OCI – Etapa 4.Fuente: INFORME PRIMER CUATRIMESTRE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN - 2025 generado por la DTSI con radicado número 3-2025-13744

Como resultado del seguimiento a las oportunidades de mejora identificadas en el Informe Rad. 3-2025-7706, en la etapa de identificación de riesgos, se evidencia que la DTSI ha venido adelantando acciones que permiten validar los lineamientos establecidos en la guía G-FI-04 V3. Sin embargo, de acuerdo con lo reportado por el proceso, respecto a la Oportunidad de Mejora N°1, "*se tiene previsto que para el segundo cuatrimestre de la vigencia 2025 se programarán mesas de trabajo orientadas a: La actualización y categorización de los activos de información de la DRFGD; La identificación, análisis y documentación de los riesgos de seguridad de la información asociados*". Esta Oficina, en el seguimiento correspondiente al segundo cuatrimestre de 2025, verificará el cumplimiento de lo señalado. En caso de no ser atendido, se dejará constancia como observación para la formulación del Plan de Mejoramiento.

4.1.5 ETAPA 5: VALORACIÓN DEL RIESGO

Como resultado de la valoración de los 33 riesgos identificados, se obtiene (6) riesgos en nivel alto, (36) en nivel moderado y (1) en nivel bajo para un total de 43 valoraciones asociadas, como se detalla:

, PROCESO	ALTO	MODERADO	BAJO	TOTAL
Acceso y Fortalecimiento a la Justicia.	0	2	1	3
Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	0	4	0	4
Atención y Relación con el Ciudadano.	0	2	0	2
Control Disciplinario.	0	2	0	2
Direccionamiento Estratégico.	1	0	0	1
Evaluación al Sistema de Control Interno.	0	3	0	3
Gestión Contractual.	0	1	0	1
Gestión de Comunicaciones Estratégicas.	0	1	0	1
Gestión de Emergencias.	0	7	0	7
Gestión de Seguridad y Convivencia.	0	7	0	7
Gestión de Tecnologías de la Información.	4	0	0	4
Gestión Estratégica del Talento Humano.	0	2	0	2
Gestión Financiera.	0	1	0	1
Gestión Integral a las Personas Privadas de la Libertad – PPL.	0	1	0	1
Gestión Jurídica.	0	1	0	1
Gestión Tecnológica de Seguridad y Emergencias.	0	2	0	2
Gestión y Análisis de la Información.	1	0	0	1
TOTAL	6	36	1	43

Tabla N. 4. Valoración de riesgos general por procesos. Elaboración OCI-Fuente: matriz de riesgos de seguridad de la información F-FI-1385

Se precisa que el total de registros reportados (43) corresponde a la cantidad de valoraciones realizadas por cada vulnerabilidad identificada por cada riesgo, algunos riesgos tienen entre 2 y 4 vulnerabilidades asociadas (ver tabla 4, casilla RIESGO # sombreado en color rojo). A continuación, se detalla la valoración de los riesgos que incluyen la evaluación de probabilidad e impacto, así como el nivel de riesgo inherente resultante:

RIESGO #	PROCESO	RIESGO	PROBABILIDAD	IMPACTO	RIESGO INHERENTE
1	Acceso y Fortalecimiento a la Justicia.	Pérdida de la Integridad	Baja	Moderado	MODERADO
2	Acceso y Fortalecimiento a la Justicia.	Pérdida de la Confidencialidad	Baja	Moderado	MODERADO
3	Acceso y Fortalecimiento a la Justicia.	Pérdida de la Integridad	Baja	Leve	BAJA
4	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	Pérdida de la Integridad	Media	Leve	MODERADO
4	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	Pérdida de la Integridad	Media	Leve	MODERADO
4	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	Pérdida de la Integridad	Media	Leve	MODERADO
4	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	Pérdida de la Integridad	Baja	Moderado	MODERADO
5	Atención y Relación con el Ciudadano.	Pérdida de la Integridad Perdida de Confidencialidad	Media	Leve	MODERADO
6	Atención y Relación con el Ciudadano.	Pérdida de la Integridad Perdida de Confidencialidad	Muy Baja	Moderado	MODERADO
7	Control Disciplinario.	Pérdida de la Integridad	Baja	Moderado	MODERADO
8	Control Disciplinario.	Pérdida de la Confidencialidad	Baja	Moderado	MODERADO
9	Direccionamiento Estratégico.	Pérdida de la Disponibilidad	Baja	Mayor	ALTO
10	Evaluación al Sistema de Control Interno.	Pérdida de la Integridad	Baja	Moderado	MODERADO
10	Evaluación al Sistema de Control Interno.	Pérdida de la Integridad	Baja	Moderado	MODERADO
11	Evaluación al Sistema de Control Interno.	Pérdida de la Integridad	Baja	Moderado	MODERADO
12	Gestión Contractual.	Pérdida de la Disponibilidad Perdida de la Integridad	Baja	Moderado	MODERADO
13	Gestión de Comunicaciones Estratégicas.	Pérdida de la Confidencialidad y Perdida de la Integridad	Muy Baja	Moderado	MODERADO
14	Gestión de Emergencias.	Pérdida de la Confidencialidad	Baja	Moderado	MODERADO
14	Gestión de Emergencias.	Pérdida de la Integridad	Baja	Moderado	MODERADO
14	Gestión de Emergencias.	Pérdida de la Disponibilidad	Muy Baja	Moderado	MODERADO
15	Gestión de Emergencias.	Pérdida de la Disponibilidad	Baja	Moderado	MODERADO
16	Gestión de Emergencias.	Pérdida de Confidencialidad, Integridad y/o disponibilidad de la información	Muy Baja	Moderado	MODERADO

RIESGO #	PROCESO	RIESGO	PROBABILIDAD	IMPACTO	RIESGO INHERENTE
17	Gestión de Emergencias.	Pérdida de la Disponibilidad	Media	Menor	MODERADO
18	Gestión de Emergencias.	Pérdida de la Disponibilidad	Baja	Menor	MODERADO
19	Gestión de Seguridad y Convivencia.	Pérdida de la Confidencialidad	Muy Baja	Moderado	MODERADO
20	Gestión de Seguridad y Convivencia.	Perdida de la Integridad y Disponibilidad	Muy Baja	Moderado	MODERADO
20	Gestión de Seguridad y Convivencia.	Perdida de la Integridad y Disponibilidad	Muy Baja	Moderado	MODERADO
21	Gestión de Seguridad y Convivencia.	Pérdida de la Confidencialidad	Baja	Moderado	MODERADO
22	Gestión de Seguridad y Convivencia.	Pérdida de la Disponibilidad	Baja	Moderado	MODERADO
23	Gestión de Seguridad y Convivencia.	Pérdida de la Confidencialidad	Baja	Moderado	MODERADO
24	Gestión de Seguridad y Convivencia.	Pérdida de la Integridad	Baja	Moderado	MODERADO
25	Gestión de Tecnologías de la Información.	Pérdida de Confidencialidad, integridad y/o disponibilidad de la información	Media	Mayor	ALTO
25	Gestión de Tecnologías de la Información.	Pérdida de Confidencialidad, integridad y/o disponibilidad de la información	Media	Mayor	ALTO
26	Gestión de Tecnologías de la Información.	Pérdida de Confidencialidad, integridad y/o disponibilidad de la información	Baja	Mayor	ALTO
26	Gestión de Tecnologías de la Información.	Pérdida de Confidencialidad, integridad y/o disponibilidad de la información	Baja	Mayor	ALTO
27	Gestión Estratégica del Talento Humano.	Pérdida de la Integridad	Baja	Moderado	MODERADO
28	Gestión Estratégica del Talento Humano.	Pérdida de la Confidencialidad	Baja	Moderado	MODERADO
29	Gestión Financiera.	Pérdida de la Integridad	Baja	Menor	MODERADO
30	Gestión Integral a las Personas Privadas de la Libertad – PPL.	Pérdida de la Disponibilidad Perdida de Confidencialidad	Baja	Moderado	MODERADO
31	Gestión Jurídica.	Pérdida de la Disponibilidad Perdida de la Confidencialidad Perdida de la Integridad	Baja	Moderado	MODERADO
32	Gestión Tecnológica de Seguridad y Emergencias.	Pérdida de Confidencialidad, Integridad y/o disponibilidad de la información	Baja	Moderado	MODERADO
32	Gestión Tecnológica de Seguridad y Emergencias.	Pérdida de Confidencialidad, Integridad y/o disponibilidad de la información	Baja	Moderado	MODERADO

RIESGO #	PROCESO	RIESGO	PROBABILIDAD	IMPACTO	RIESGO INHERENTE
33	Gestión y Análisis de la Información.	Pérdida de la Integridad	Baja	Mayor	ALTO

Tabla N. 5. Valoración de riesgos de seguridad de la información a detalle Elaboración Oficina de Control Interno, Fuente: matriz de riesgos de seguridad de la información F-FI-1385.

En consecuencia, aunque se están valorando los riesgos con un resultado de (43) valoraciones de riesgo inherente no son consistentes con el número de riesgos identificados por proceso, ver **(Observación 2).**

4.1.6 ETAPA 6: CREACIÓN DE CONTROLES:

Del análisis efectuado se observó que los controles identificados guardan coherencia con la estructura establecida para la construcción de un control, según lo indicado en el numeral 9.7.1 de la Guía de Administración de Riesgos:

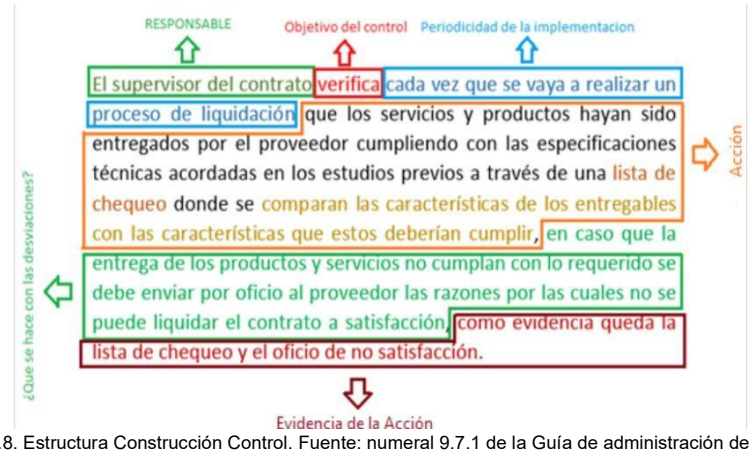


Imagen N.8. Estructura Construcción Control. Fuente: numeral 9.7.1 de la Guía de administración de riesgos

Se evidenció que la descripción de los controles cumplen con los criterios estructurales que enfatiza la guía como (responsable, objetivo del control, periodicidad de la implementación, acción, que se hace en caso de desviación y cuál es la evidencia de la acción.)

Respecto al último criterio que señala "*incluir la acción a tomar en caso de presentarse una desviación*", en el cual, se identifican las situaciones que generan diferencias entre el resultado esperado y el obtenido, así como las acciones correspondientes para su tratamiento, si bien se evidencia cumplimiento del lineamiento señalado en la guía, se observan aspectos susceptibles de mejora, como se detalla con el siguiente ejemplo:

RIESGO #	PROCESO	CONTROL #	CONTROL	SEGUIMIENTO OCI
4	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	1	El supervisor de contratos valida de forma mensual, que las fallas en la producción de informes de gestión de la plataforma se reporten a través de la mesa de servicio con el fin que este sea escalado al personal encargado de realizar las actualizaciones y/o mejoras al sistema (SIMBA), como evidencia se entrega el reporte mensual de fallas de producción el cual se solicitara 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.	En este caso específico, la instrucción de "*se deberá informar al Director*", no incluye detalles sobre las acciones posteriores para su tratamiento que permitan garantizar el cumplimiento de la actividad generada **que corrija la desviación detectada.**

Tabla N. 6. Valoración de riesgos de seguridad de la información a detalle. Fuente: matriz de riesgos de seguridad de la información F-FI-1385

Se recomienda revisar todos los controles y fortalecer la descripción de las acciones posteriores que garanticen la ejecución de la actividad de control, especificando acciones concretas que aseguren la corrección oportuna y efectiva de la desviación detectada.

De manera complementaria, en seguimiento de la gestión realizada con base en las observaciones y recomendaciones emitidas por la Oficina de Control Interno a través del Informe de Seguimiento a los Riesgos de seguridad de la Información tercer cuatrimestre 2024, Radicado N. 3-2025-7706 en la etapa de creación de controles, se obtuvo el siguiente resultado:

OPORTUNIDAD DE MEJORA	REPORTE DE LA SEGUNDA LÍNEA DE DEFENSA (DTI)	SEGUIMIENTO TERCERA LÍNEA DE DEFENSA (OFICINA DE CONTROL INTERNO)
Oportunidad de Mejora N°4: 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. 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.	Se informa que se programarán para el segundo y tercer cuatrimestre de la vigencia 2025, las respectivas mesas de trabajo con las áreas responsables de los procesos, con el fin de: • Revisar los controles existentes en la matriz F-FI-1385. • Clasificarlos adecuadamente según su tipología (automáticos o manuales). • Ajustar o incorporar nuevos controles conforme a los riesgos identificados.	**Resultado:** El proceso indica que se programará para el segundo y tercer cuatrimestre. Por lo anterior, **se reitera la Oportunidad de Mejora N°4** **Recomendación:** Se recomienda establecer un plan de trabajo con responsables y tiempos definidos para implementar las acciones previstas a ejecutar "*Revisar los controles existentes en la matriz F-FI-1385 y clasificarlos según su tipología (automáticos o manuales), Ajustar o incorporar nuevos controles conforme a los riesgos identificados*". Además, es fundamental realizar un seguimiento periódico para verificar el cumplimiento de las medidas adoptadas y garantizar la mejora continua en los procesos.

Tabla N. 7. Gestión Adelantada frente a las Oportunidades de Mejora emitidas por OCI – Etapa 6.Fuente: INFORME PRIMER CUATRIMESTRE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN - 2025 generado por la DTSI con radicado número 3-2025-13744

Esta Oficina, en el seguimiento correspondiente al segundo cuatrimestre de 2025, verificará el cumplimiento de lo señalado por el proceso.

4.1.7 ETAPA 7: TRATAMIENTO DEL RIESGO RESIDUAL.

Todos los riesgos identificados en la Secretaría Distrital de Seguridad, Convivencia y Justicia cuentan con un tratamiento residual, independientemente de la Zona de Riesgo asignada. Sin embargo, se evidenció que en la matriz de riesgos de seguridad de la información F-FI-1385, específicamente en la hoja "TRATAMIENTO DE RIESGO RESIDUAL", la totalidad de los 33 riesgos establecidos fueron categorizados con la opción "REDUCIR EL RIESGO", lo cual sugiere una homogeneidad en la estrategia de tratamiento que podría requerir un análisis más diferenciado según la naturaleza de cada riesgo, adicionalmente se observa que una vez aplicados los controles todos los riesgos disminuyen y pasan a la zona BAJA.

A continuación, se ilustra el resultado de la zona de riesgo residual por procesos:

, PROCESO	RIESGO RESIDUAL		
	ALTO	MODERADO	BAJO
Acceso y Fortalecimiento a la Justicia.	0	0	3
Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	0	0	4
Atención y Relación con el Ciudadano.	0	0	2
Control Disciplinario.	0	0	2
Direccionamiento Estratégico.	0	0	1
Evaluación al Sistema de Control Interno.	0	0	3
Gestión Contractual.	0	0	1
Gestión de Comunicaciones Estratégicas.	0	0	1
Gestión de Emergencias.	0	0	7
Gestión de Seguridad y Convivencia.	0	0	7
Gestión de Tecnologías de la Información.	0	0	4
Gestión Estratégica del Talento Humano.	0	0	2
Gestión Financiera.	0	0	1
Gestión Integral a las Personas Privadas de la Libertad – PPL.	0	0	1
Gestión Jurídica.	0	0	1
Gestión Tecnológica de Seguridad y Emergencias.	0	0	2
Gestión y Análisis de la Información.	0	0	1
TOTAL	0	0	43

Tabla N. 8. Valoración riesgo residual por procesos. Elaboración OCI-Fuente: matriz de riesgos de seguridad de la información F-FI-1385

4.1.8 ETAPA 8: MONITOREO, REVISIÓN Y REPORTE.

En relación con la evaluación realizada y presentada mediante el radicado No. 3-2025-7706, emitido por la Oficina de Control Interno y correspondiente al *"Informe de seguimiento a riesgos de seguridad de la información - tercer cuatrimestre de 2024",* se evidenció la realización de mesas de trabajo con

las áreas involucradas, con el propósito de atender las observaciones y recomendaciones. Estas acciones se encuentran documentadas en el Informe radicado No. 3-2025-19176, y fueron validadas con las evidencias presentadas por la Dirección de Tecnologías y Sistemas de la Información (DTSI) para el primer cuatrimestre de 2025.

A continuación, la Oficina de Control Interno realiza el seguimiento y la evaluación de la ejecución de los controles establecidos en la Matriz de Riesgos de Seguridad de la SDSCJ. En este proceso, se verificaron los soportes allegados por la primera línea de defensa, depositados en el repositorio dispuesto por la segunda línea de defensa (DTSI), obteniendo el siguiente resultado:

RIESGO #	PROCESO	CONTROL #	CONTROL	SOPORTE	SEGUIMIENTO OCI	CUMPLE
1	Acceso y Fortalecimiento a la Justicia.	1	El Líder Funcional de la herramienta SIDIJUS, verifica de forma cuatrimestral la asignación de permisos de usuario y roles de la plataforma con el fin de validar que solo las personas autorizadas se encuentre con usuario activo de acuerdo a las responsabilidades asignadas por la dirección, como evidencia envía correo electrónico y/o documento oficial con el listado de usuarios activos al Director (a) de Acceso a la Justicia con el tipo de acceso y permisos a la información, en caso que los usuarios no tengan autorización se retiraran permisos de acceso y se informara de las acciones al Jefe de la Dirección.	Soportes de la documentación entregada en los repositorios SharePoint disponibles para el área.	Se evidenció la ejecución de la actividad de control mediante el listado de usuarios SIDIJUS 2025, así como a través del correo electrónico enviado al Director de Acceso a la Justicia el 23 de abril de 2025, en el cual se informó sobre la depuración y actualización correspondientes al primer cuatrimestre de 2025.	SI
2	Acceso y Fortalecimiento a la Justicia.	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.	Comunicación oficial y/o correo electrónico	El proceso aportó el correo electrónico del día 23/04/2025, mediante el cual se solicita confirmar si se tiene acceso a la carpeta "Informes de Gestión 2025". Sin embargo, no se aportó evidencia que respalde la verificación de permisos derecho de acceso a formularios conforme a lo establecido en el control, así como, no se aporta soporte documental de la acción ante la desviación, el cual indica que: "*En caso de que los usuarios no tengan autorización, se retirarán los permisos de acceso y se informará de las acciones al Jefe de área*". **Recomendación:** Aportar evidencia de la verificación de permisos y de las acciones tomadas en caso de accesos no autorizados, de conformidad con los lineamientos del control establecido.	NO

RIESGO #	PROCESO	CONTROL #	CONTROL	SOPORTE	SEGUIMIENTO OCI	CUMPLE
3	Acceso y Fortalecimiento a la Justicia.	1	El profesional responsable del reporte de riesgos y controles de Seguridad de la Información debe validar mensualmente la ejecución del plan de copias de respaldo de las bases de datos de la Dirección de Responsabilidad Penal Adolescente (DRPA), asegurando que se cumplan los pasos y plazos establecidos para garantizar la integridad de la información, como evidencia se presenta al director el comunicado oficial y/o correo electrónico sobre la ejecución del plan de copias de respaldo de las bases de datos. En caso de no realizar las actividades establecidas en el plan, se debe informar al director a través de correo electrónico sobre los motivos y las acciones para cumplir con el mismo.	Comunicación oficial y/o correo electrónico	Se evidenció la ejecución de la actividad de control con los informes de seguimiento mensuales sobre la correcta ejecución de las copias de respaldo, correos y reportes de los meses de enero, febrero, marzo y abril de 2025.	SI
4	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	1	El supervisor de contratos valida de forma mensual, que las fallas en la producción de informes de gestión de la plataforma se reporten a través de la mesa de servicio con el fin que este sea escalado al personal encargado de realizar las actualizaciones y/o mejoras al sistema (SIMBA), como evidencia **se entrega el reporte mensual de fallas de producción** el cual se solicitara 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.	Comunicación oficial y/o correo electrónico	No se aportó evidencia que respalde la ejecución de la actividad de control como el reporte mensual de fallas de producción, el cual se solicita mediante correo electrónico o comunicado oficial a la DTSI, adicionalmente, no se aportó evidencia de la acción ante la desviación "*en caso de no entregar el reporte se debe informar al director de Bienes con las acciones para dar cumplimiento*". **Recomendación:** Establecer mecanismos que aseguren la trazabilidad y documentación de la ejecución de las actividades de control, tales como el reporte mensual de fallas de producción. Adicionalmente, se sugiere documentar las acciones tomadas en caso de incumplimientos, de conformidad con lo establecido en el control.	NO
4	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	2	El administrador de la plataforma SIMBA, realiza solicitud de forma mensual por correo electrónico y/o comunicado oficial a los talleres sobre el cambio de contraseña para la plataforma de acceso (SIMBA) de acuerdo a las funciones habilitadas para cada taller, En caso de no realizar la solicitud dentro de la vigencia del mes se informara al director de bienes los motivos y las acciones para enviar la notificación, como evidencia se entregara la solicitudes de cambio de contraseña a los talleres.	Comunicación oficial y/o correo electrónico	La evidencia aportada no permite verificar la ejecución de la actividad de control, debido a que no se aportó evidencia que dé cuenta de las solicitudes mensuales comunicando los talleres, tan solo se evidencian correos en donde se solicita cambios de contraseñas uno del mes de diciembre 2024 que no aplicaría y otro en el mes febrero 2025; adicionalmente, no se aportó evidencia de la acción ante la desviación ***"****En caso de no realizar la solicitud dentro de la vigencia del mes se informará al director de bienes los motivos y las acciones para enviar la notificación, como evidencia se entregara la solicitudes de cambio de contraseña a los talleres*".	NO

RIESGO #	PROCESO	CONTROL #	CONTROL	SOPORTE	SEGUIMIENTO OCI	CUMPLE
					Recomendación: Se requiere establecer un registro formal y verificable de las solicitudes mensuales a los talleres, así como documentar las acciones tomadas ante incumplimientos, conforme a lo definido en el control.	
4	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	3	El administrador de la plataforma SIMBA, de forma cuatrimestral realiza capacitación y/o sensibilización a funcionarios, contratistas y terceros sobre el correcto uso de la plataforma SIMBA de acuerdo a las funcionalidades y servicios, como soporte de la evidencia se dejará las listas de asistencia y/o soportes documentales de las capacitaciones, para los casos que el personal no asista se reprogramará una nueva sesión de capacitación	Listas de Asistencia y/o soportes	La evidencia aportada no permite verificar la ejecución de la actividad de control, debido a que se observa un acta de asistencia correspondiente al mes de octubre de 2024, la cual no aplica para el periodo evaluado, y otra del 31 de enero de 2025 relacionada con la capacitación sobre SIMBA dirigida a supervisores y apoyos técnicos del **Grupo Movilidad**; sin embargo, no se evidencia la participación de los demás funcionarios y contratistas, adicional la periodicidad es cuatrimestral y no hay registros. **Recomendación:** Se hace necesario asegurar el cumplimiento de la actividad de control mediante la programación y documentación oportuna de las capacitaciones conforme a la periodicidad establecida. Asimismo, se debe garantizar la participación de todos los funcionarios y contratistas, dejando evidencia formal y completa de asistencia para el periodo evaluado.	NO
	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	4	El coordinador de cada grupo Funcional de forma semestral valida la disponibilidad de personal asignado para el cumplimiento de las tareas dentro de la operación del sistema SIMBA, de lo cual entregara al director del área una proyección de las necesidades de operación y la continuidad del personal idóneo para el cumplimiento adecuado de las funciones, como evidencia se entrega la proyección del personal requerido, en caso de no contar con el personal necesario para la operación se solicitara mediante comunicado oficial al Director del área, de acuerdo a la novedad	Proyección de personal requerido	Se reportó que durante este periodo no se dio aplicación a la actividad de control, toda vez que es semestral y será reportado para el segundo cuatrimestre del 2025.	N/A

RIESGO #	PROCESO	CONTROL #	CONTROL	SOPORTE	SEGUIMIENTO OCI	CUMPLE
5	Atención y Relación con el Ciudadano.	1	El responsable del registro documental, cuatrimestralmente realiza la verificación de la información recibida por parte de los reportes del sistema de gestión documental - SIGA, validando la integridad de la información y alimentando con esta el formato matriz de trazabilidad PQRS, como evidencia se entrega el formato diligenciado. En caso de que la información no este exacta y completa se deberá emitir correo electrónico y/o documento oficial a las partes interesadas solicitando las correcciones del caso.	Formato Diligenciado	Se evidenció la ejecución de la actividad con la MATRIZ DE TRAZABILIDAD DE PQRSDF CIUDADANAS F-AR-1478 V.1 diligenciada para los meses de enero, febrero, marzo y abril de 2025.	SI
6	Atención y Relación con el Ciudadano.	1	El responsable del equipo de cobro persuasivo, semestralmente, verifica con el personal de soporte técnico los usuarios activos en el sistema de procesamiento de información de los expedientes de cobro persuasivo de acuerdo a los roles y responsabilidades asignados, 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.	Comunicación oficial y/o comunicación vía Teams	Se evidenció la ejecución de la actividad con el correo enviado el día 24 de abril, solicitando reporte de los usuarios activos COPE.	SI
7	Control Disciplinario.	1	El auxiliar administrativo de la oficina de Control Disciplinario interno designado, previa autorización del jefe OCDI, realiza cada vez que se requiera la autorización de acceso a los usuarios a la información, otorgando los permisos de lectura y/o edición de acuerdo al requerimiento, como soporte se contará con la solicitud de permisos a través de correo electrónico, en caso de no contar con solicitud o requerimiento previo no se dará autorización de ingreso a la información.	Solicitud de permisos a través de correo electrónico	Se evidenció la ejecución de la actividad con dos correos electrónicos asunto: Autorización ingreso a las bases de la OCDI.	SI
8	Control Disciplinario.	2	El auxiliar administrativo de la oficina de Control Disciplinario Interno asignado, de forma cuatrimestral verifica los permisos de derecho de acceso a los expedientes de Investigaciones Disciplinarios digitales, de acuerdo con los roles y responsabilidades asignados para tal fin, como soporte de la revisión envía comunicación oficial y/o correo electrónico al Jefe de OCDI informando los usuarios que cuentan con acceso y el tipo de acceso a la información, en caso que los usuarios no tengan autorización se retiraran permisos de acceso y se informara de las acciones al Jefe de OCDI.	Comunicación oficial y/o correo electrónico	Se evidenció la ejecución de la actividad de control con el reporte de los usuarios actualmente autorizados y la aprobación por parte del Jefe de la Oficina Control Interno Disciplinario.	SI

RIESGO #	PROCESO	CONTROL #	CONTROL	SOPORTE	SEGUIMIENTO OCI	CUMPLE
9	Direccionamiento Estratégico.	1	El profesional asignado por la Oficina Asesora de Planeación para las publicaciones en el sitio web trimestralmente realiza el seguimiento y monitoreo a las publicaciones que se deben realizar por cada periodo en el sitio web de la Entidad mediante correo electrónico a los responsables con base al esquema de publicación. En caso de no recepcionar la información para publicación se deberá informar al Jefe de la Oficina de Planeación. Como evidencia quedara el correo de notificación y el esquema de publicación.	Correo de Notificación y esquema de publicación	Se evidenció la ejecución de la actividad de control mediante el monitoreo del botón de transparencia correspondiente al primer trimestre de 2025. Asimismo, se presentó el esquema de publicación y los correos electrónicos enviados, con base en dicho esquema.	SI
10	Evaluación al Sistema de Control Interno.	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.	Reporte de sistema de información	Se evidenció la ejecución de la actividad del control con las evidencias 001. R10-C1-001-F-SM-951-SegPMICB-2025 y el pantallazo del repositorio SharePoint de la Oficina de Control Interno.	SI
10	Evaluación al Sistema de Control Interno.	2	El profesional designado por la jefatura de la OCI semestralmente solicita a las dependencias vía correo electrónico la información de los enlaces responsables que ingresarán a la herramienta en la cual se realiza reporte del plan de mejoramiento institucional, para garantizar que los usuarios autorizados correspondan con los designados. En caso de identificar un usuario no autorizado, inmediatamente se restringe el acceso por medio de solicitud a la DTSI. Como evidencia se presentan el correo enviado a las dependencias, las respuestas de estas, la solicitud a la DTSI del bloqueo y la respuesta de la acción ejecutada en la herramienta por parte del administrador de la plataforma.	Correo o Memorando	Se evidenció la ejecución de la actividad del control con el memorando con radicado número 3-2025-187, emitido por la Oficina de Control Interno en donde indica que cada dependencia realizó la designación del profesional para el reporte de los planes de mejoramiento institucionales el pasado 13 de diciembre de 2024, e indica realizar el reporte y cargue de soportes documentales asociado a las acciones de mejora en estado “Abierta en Términos” que se encuentran suscritas en el Plan de Mejoramiento de la entidad.	SI
11	Evaluación al Sistema de Control Interno.	1	El profesional de la Oficina de Control Interno de forma trimestral descarga el reporte del sistema de información en el que se genere el reporte a los planes de mejoramiento por procesos (internos) y se cargara este archivo en el repositorio SharePoint disponible para la Oficina de Control Interno. en caso de no poder descargar el reporte se solicita a la DTSI se genere el reporte correspondiente por parte del administrador de la herramienta.	Reporte de planes de mejoramiento por procesos	Se evidenció la ejecución de la actividad de control con el reporte R11-C1-000. F-SM-951-HojaTrabajo-2025 y la pantalla del cargue en el SharePoint de la Oficina de Control Interno.	SI

RIESGO #	PROCESO	CONTROL #	CONTROL	SOPORTE	SEGUIMIENTO OCI	CUMPLE
12	Gestión Contractual.	1	El responsable del equipo de archivo de la Dirección Jurídica y Contractual anualmente realiza la intervención documental de los expedientes en referencia a la completitud y correspondencia de archivos de los expedientes que se maneja en el área, como evidencia se genera el inventario documental de la DJC. En caso de no entregar el inventario documental a las instancias correspondientes se debe informar al Director(a) Jurídico(a) y Contractual de las acciones para dar cumplimiento.	Inventario Documental de la DJC	Se evidenció la ejecución de la actividad de control con el reporte documental del periodo enero a abril de 2025 correspondiente a la información de Archivo Contratos de Jurídica.	SI
13	Gestión de Comunicaciones Estratégicas.	1	El Líder Digital de la Oficina Asesora de Comunicaciones realiza de forma trimestral y/o cuando halla novedades con el personal encargado de las redes sociales, la actualización de las contraseñas de acceso a las diferentes cuentas de redes sociales de la Entidad , como evidencia se debe enviar comunicación oficial y/o correo electrónico al Jefe de la OAC evidenciando el cambio de contraseña, En caso de no realizar la actividad el jefe de la OAC tomará las acciones necesarias para que se ejecute el control, como evidencia se presenta el comunicado oficial enviado por el líder Digital.	Comunicación oficial y/o correo electrónico	Se evidenció la ejecución de la actividad con correo electrónico que evidencia el cambio de contraseñas de las Redes Sociales de la SCJ.	SI
14	Gestión de Emergencias.	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.	Comunicado Oficial sobre el Seguimiento a la Operación y Acciones Realizadas.	La evidencia aportada no permite verificar la ejecución completa de la actividad de control, ya que el proceso presentó los informes de gestión y operación correspondientes a los meses de enero y febrero de 2025, así como el de diciembre de 2024, este último no aplicable al periodo evaluado. También se aportaron tres informes de apoyo y dos de supervisión; sin embargo, se encuentran pendientes los correspondientes a los meses de marzo y abril de 2025. Adicionalmente, no se evidencian las gestiones realizadas ante la ausencia de reportes por parte del operador tecnológico, tal como lo indica el control: *'En caso de no contar con los reportes que entrega el operador tecnológico, se realizarán las gestiones pertinentes mediante comunicado oficial y/o correo electrónico sobre la solicitud de información".* **Recomendación:** Fortalecer el seguimiento a la ejecución de la actividad de control mediante la presentación completa y oportuna de los informes de operación, apoyo y supervisión correspondientes a cada periodo. Asimismo, se sugiere	NO

RIESGO #	PROCESO	CONTROL #	CONTROL	SOPORTE	SEGUIMIENTO OCI	CUMPLE
					documentar las gestiones realizadas en caso de ausencia de reportes por parte del operador tecnológico, conforme al procedimiento establecido.	
14	Gestión de Emergencias.	2	El Grupo Operaciones C-4, mensualmente verifica la disponibilidad de personal asignado para el cumplimiento de las tareas dentro de la operación del NUSE123, de lo cual entregara una proyección sobre ausencia de personal y necesidades de operación. como evidencia se entregará matriz proyección de turnos operación de C4, para toma de decisiones. en caso de no contar con el personal necesario de operación envían un correo al jefe de C4, con la novedad.	Proyección Sobre Ausencia Personal y Necesidades de Operación.	Se evidenció la ejecución de la actividad de control con el correo que da cuenta de la Proyección Operativa NUSE 123 de los meses enero, febrero, marzo y abril de 2025	SI
14	Gestión de Emergencias.	3	El grupo de entrenamiento C-4, semestralmente, realiza capacitación y /o sensibilización a funcionarios y contratistas sobre el correcto uso de contraseñas de acuerdo con lo establecido en el manual de seguridad y privacidad de la información de la Entidad, como soporte de la evidencia se dejarán las listas de asistencia y documentos de apoyo de las capacitaciones, para los casos que personal no asista se procede con la reprogramación de una nueva sesión de capacitación.	Listas de Asistencia y documentos de apoyo a las capacitaciones	Se evidenció la ejecución de la actividad de control con los listados de asistencia de las capacitaciones efectuadas en los meses de enero, febrero, marzo y abril de 2025, así como los materiales de capacitación.	SI
15	Gestión de Emergencias.	1	El grupo de seguimiento de infraestructura tecnológica del C-4, 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.	Informes técnicos de funcionamiento de UPS	Se evidenció la ejecución de la actividad de control con los Informes PRTG 2855 - Informe UPS breve semanal - Generados 2025 de los meses enero, febrero, marzo y abril.	SI

RIESGO #	PROCESO	CONTROL #	CONTROL	SOPORTE	SEGUIMIENTO OCI	CUMPLE
16	Gestión de Emergencias.	1	El jefe del C4 delega a la empresa contratista el mantenimiento y operación del sistema de comunicaciones. Estas actividades se registran en informes de gestión de la empresa contratista recibidos de forma mensual evidenciando la operación del sistema de comunicaciones controlada por ANS, que en caso de estar por debajo de umbral se penaliza económicamente. las Evidencia corresponde al Informe mensual de la empresa contratista. El cargue de las evidencias se hará trimestralmente.	Informe Mensual de Empresa Contratista	Se evidenció la ejecución de la actividad de control con los informes de actividades Nos. 9,10,11 y 12 del Contrato 760 de 2025	SI
17	Gestión de Emergencias.	1	El coordinador de la Sala SOARS, realiza de forma mensual el cargue de la copia de seguridad de la base de datos incidentes SOARS en el repositorio establecidos en el C-4, en caso de no realizar la copia de seguridad se debe informar al jefe de C-4 los motivos y las acciones para el cargue de esta información, como evidencia se envía correo electrónico y/o comunicado oficial al líder del C-4.	Correo Electrónico	Se evidenció el correo electrónico del cargue de la información de SOARS correspondiente al primer cuatrimestre del año en el SharePoint, No obstante, al no aportar el link de acceso no se puede validar la existencia de la copia de seguridad de la base de datos incidentes SOARS en el repositorio establecido. **Recomendación**: Se sugiere que, al momento de cargar información en el repositorio de SharePoint, se incluya de forma explícita el enlace de acceso al archivo o carpeta correspondiente. Esto permitirá validar la existencia de la copia de seguridad de la base de datos de incidentes SOARS y garantizará la trazabilidad y disponibilidad de la información cargada para su revisión y auditoría.	NO
18	Gestión de Emergencias.	1	El coordinador de la Sala SOARS, realiza de forma mensual el cargue de la copia de seguridad de la bitácora de transferencia de mando del área de seguimiento en el repositorio establecidos en el C-4, en caso de no realizar la copia de seguridad se debe informar al jefe de C-4 los motivos y las acciones para el cargue de esta información, como evidencia se envía correo electrónico y/o comunicado oficial al líder del C-4.	Correo Electrónico	Aunque el proceso reporta el correo electrónico del cargue de la información de SOARS correspondiente al primer cuatrimestre del año en el SharePoint. No aportó la evidencia que permita validar la realización del cargue de la copia mensual de seguridad de la bitácora de transferencia de mando del área de seguimiento en el repositorio establecidos en el C-4 **Recomendación:** Adjuntar evidencia verificable del cargue mensual de la copia de seguridad de la bitácora de transferencia de mando del área de seguimiento en el repositorio C-4, ya que el correo reportado no permite validar dicha acción.	NO

RIESGO #	PROCESO	CONTROL #	CONTROL	SOPORTE	SEGUIMIENTO OCI	CUMPLE
19	Gestión de Seguridad y Convivencia.	1	El responsable de almacenamiento de las actas debe asegurar que los permisos otorgados a los usuarios sobre estos documentos, sean actualizados y/o retirados semestralmente, de acuerdo con los roles y permisos de cada funcionario que accede a la información, debe quedar como evidencia correo electrónico enviado al líder del proceso evidenciando los funcionarios que tienen acceso y el tipo de permiso que tienen (lectura, escritura, o ambos) En caso de que el responsable de almacenamiento de las actas no tenga permisos de gestión sobre la carpeta, deberá solicitarlos al secretario.	Correo Electrónico	Se evidenció la ejecución de la actividad del control con el correo electrónico del día 30/04/2025 Asunto: Control de riesgo de seguridad de la información.	SI
20	Gestión de Recursos Físicos al Servicio de la Entidad.	1	El responsable de gestión de la información de Subsecretaría de Seguridad y convivencia debe solicitar Cuatrimestralmente ante la DTSI de la Entidad, el reporte de usuarios y roles activos de la plataforma designada, para verificar que los permisos otorgados a los usuarios sobre esta información sean los correctos, debe quedar como evidencia correo electrónico enviado a líder del proceso evidenciando los funcionarios y contratistas que tienen acceso y el tipo de permiso que tienen (lectura, escritura, o ambos) En caso de que exista usuarios con permisos no autorizados o retirados aún activos en la plataforma, se deberán corregir o solicitar el retiro al responsable de la plataforma en DTSI e informar al líder de proceso mediante correo electrónico y/o comunicado oficial.	Reporte de usuarios y roles de plataforma asignada	Se evidenció la ejecución de la actividad de control con el correo informando la verificación de usuarios activos y roles en progressus, así como el reporte de usuarios y roles.	SI
20	Gestión de Seguridad y Convivencia.	2	El líder operativo de la Subsecretaría de seguridad y convivencia, evalúa de forma cuatrimestral a través de mesas de trabajo la necesidad de actualizar la guía para el uso adecuado de la plataforma; como evidencia se contara con el correo electrónico y/o acta de reunión donde se especifica la viabilidad de la actualización del documento y el tiempo de ajuste de la misma, en caso de no realizarse las mesas de trabajo de actualización de la guía se contara con comunicación formal al líder del proceso y se debe reprogramar dentro del mes posterior.	Correo Electrónico y/o acta de reunión	Se evidencia la ejecución de la actividad con el acta de reunión de abril tema: Revisión y ajustes Guía para el Registro y Validación de Actividades en Progressus G-GS-06	SI

RIESGO #	PROCESO	CONTROL #	CONTROL	SOPORTE	SEGUIMIENTO OCI	CUMPLE
21	Gestión de Seguridad y Convivencia.	1	El (a) Director (a) de Seguridad, verifica en reunión Cuatrimestral, que los documentos se almacenen en un sitio seguro dispuesto por la Entidad para restringir el acceso y uso únicamente para los usuarios autorizados, por medio de acta valida que el proceso de custodia y confidencialidad del documento final se realizó adecuadamente y/o de la aplicación de los correctivos necesarios, en caso de requerirse; en caso de no realizar la verificación se debe reprogramar dentro del mes posterior.	Acta	Se evidenció la ejecución de la actividad de control con el acta de reunión tema: Control y Seguimiento al cargue de documentación Sitio Share Point 220 Dirección de Seguridad correspondiente al primer cuatrimestre de 2025, con el fin de dar cumplimiento a criterios de custodia y confidencialidad de la información generada por la dependencia.	SI
22	Gestión de Seguridad y Convivencia.	1	El responsable de validar las Actas de los Consejos Locales de Seguridad verifica mensualmente que las actas de meses anteriores hayan sido aprobadas y cargadas en la plataforma dispuesta para ello, también verifica que se haya cargado al menos el borrador de las actas del mes en revisión. En caso de evidenciar consejos cuyas actas aún no han sido aprobadas o el borrador no fue realizado, genera un reporte y solicita a los responsables de la secretaría técnica del Consejo Local de Seguridad, que realicen la subsanación correspondiente, las evidencias se cargaran de forma Cuatrimestral.	Correo electrónico	Se evidenció la ejecución de la actividad de control con los correos electrónicos que relacionan la disponibilidad de las actas de los Consejos Locales de Seguridad - CLS - Control periodo de validación enero a abril 2025.	SI
23	Gestión de Seguridad y Convivencia.	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.	Actualización tabla de avance	Se reportó que durante este periodo no se dio aplicación a la actividad de control, debido a que la periodicidad del control es semestral, por lo cual se reportará oportunamente.	N/A

RIESGO #	PROCESO	CONTROL #	CONTROL	SOPORTE	SEGUIMIENTO OCI	CUMPLE
24	Gestión de Seguridad y Convivencia.	1	El responsable de gestión de la información de la Subsecretaría de Seguridad y Convivencia verifica de forma cuatrimestral que al menos el 80% de los registros del formulario correspondan con las evidencias de las actividades realizadas durante el periodo, como evidencia se entrega la tabla de verificación de actualización de registros. En caso de no cumplir con el porcentaje establecido se requerirá por correo electrónico a los responsables de las actividades para realizar la verificación respectiva.	Tabla de verificación de correspondencia de registro.	La evidencia aportada no permite verificar la ejecución de la actividad, ya que el proceso únicamente presentó un correo de solicitud para adelantar las acciones necesarias orientadas al registro de la información pendiente en el formulario SURVEY 123. Por otra parte, se encuentra pendiente la entrega de la Tabla de Verificación de Correspondencia, la cual es fundamental para confirmar el avance y cumplimiento de la actividad correspondiente. **Recomendación:** Se sugiere complementar la evidencia con documentación que respalde la ejecución efectiva de la actividad, incluyendo la Tabla de Verificación de Correspondencia debidamente actualizada y validada por los responsables del proceso.	NO
25	Gestión de Tecnologías de la Información.	1	El responsable de sistema de información y/o infraestructura Tecnológica verifica de forma cuatrimestral el seguimiento al plan de trabajo de versionamiento de los ambientes de pruebas y productivos asociados a los sistemas de información, en caso de no realizar el seguimiento se debe evidenciar las causas de no realizar las actividades del plan a través de actas, informes y/o correos electrónicos, como evidencia de la ejecución del control se contara con los avances de las actividades del plan mediante bitácoras de actividades, actas y/o comunicado oficial.	Reporte del Seguimiento al Plan o verificación de versiona miento en el ambiente de desarrollo y producción	Se evidencia la ejecución de la actividad de control con el documento en Excel “plan de trabajo” que incluye las actividades desplegadas por sistema.	SI
25	Gestión de Tecnologías de la Información.	2	El responsable de sistema de información realiza seguimiento cuatrimestral a la ejecución del plan de actualización documental de la arquitectura de los sistemas de información, en caso de no contar con el seguimiento trimestral al plan de actualización documental de la arquitectura, se deberá contar con los manuales técnicos actualizados de cada uno de los sistemas de información. Como evidencia de la ejecución del control se contará con el reporte de seguimiento al plan o con los manuales técnicos de los sistemas	Reporte del Seguimiento al Plan o manuales técnicos de los sistemas	Se evidencia la ejecución de la actividad de control con todos los manuales técnicos, Apelaciones, SIGA-SGDA, LICO, ARGOS, ORFEO, SCP Videovigilancia, Progressus, Limay, SIMBA, Casa libertad, SIRPA, Sitio web, SISIPEC, SAE, SAI, SISCO, OPGET, PREDIS, entre otros.	SI

RIESGO #	PROCESO	CONTROL #	CONTROL	SOPORTE	SEGUIMIENTO OCI	CUMPLE
26	Gestión de Tecnologías de la Información.	1	El responsable de infraestructura define el mecanismo seguro y estandarizado para la gestión segura de credenciales de administración en la infraestructura tecnológica, así como **el seguimiento trimestral al cumplimiento de los mecanismos establecidos**, en caso de no contar con el seguimiento trimestral a los mecanismos establecidos, se contará con comunicación formal al Director de Tecnologías informando las alternativas adoptadas. Como evidencia de la ejecución del control se contará con el mecanismo de gestión segura de contraseñas o comunicado formal.	Mecanismo de gestión segura de contraseñas o comunicado oficial	La evidencia aportada no permite verificar la ejecución de la actividad de control en su totalidad, debido a que si bien el proceso aportó un documento titulado Mecanismo de gestión segura de contraseñas, que tiene como objetivo "*Establecer y mantener un sistema robusto y eficiente para la gestión de credenciales de administración que garantice la seguridad, integridad y accesibilidad de los sistemas de información de la SDSCJ,* no se aportó evidencia que dé cuenta del seguimiento trimestral al cumplimiento de los mecanismos establecidos, asimismo, no se tienen registros de la acción ante la desviación en caso de no contar con el seguimiento. **Recomendación**: se hace necesario ajustar lo que indica el soporte de la actividad de control, toda vez, que es necesario incluir el reporte con el seguimiento trimestral.	NO
26	Gestión de Tecnologías de la Información.	2	El responsable de infraestructura tecnológica realiza seguimiento trimestral al funcionamiento de herramientas de seguridad informática que protegen la información de la SDSCJ, en caso de no hacer seguimiento al funcionamiento se contara con comunicación formal al Director de Tecnologías informando las alternativas adoptadas. Como evidencia de la ejecución del control se contará con el reporte de rendimiento de la infraestructura de seguridad o el comunicado formal.	Reporte de rendimiento de la infraestructura de seguridad o comunicado oficial	Se evidenció la ejecución de la actividad con el reporte performance de rendimiento.	SI
27	Gestión Estratégica del Talento Humano.	1	El Profesional especializado responsable de nómina, solicita a la DTSI en caso de una novedad, el permiso y/o retiro de acceso de usuarios autorizados de forma permanente al sistema de información y/o repositorios asignados para el manejo de esta información, como evidencia se tendrán las comunicaciones de solicitud y/o retiro de acceso de usuarios. en caso de que los permisos no sean gestionados correctamente se reitera la solicitud mediante correo electrónico a la mesa de servicio con los ajustes requeridos. El cargue de evidencia se realizará de forma cuatrimestral.	comunicación de solicitud y/o retiro de acceso de usuarios	Se evidenció la ejecución de la actividad con el correo de solicitud de eliminación de usuarios.	SI

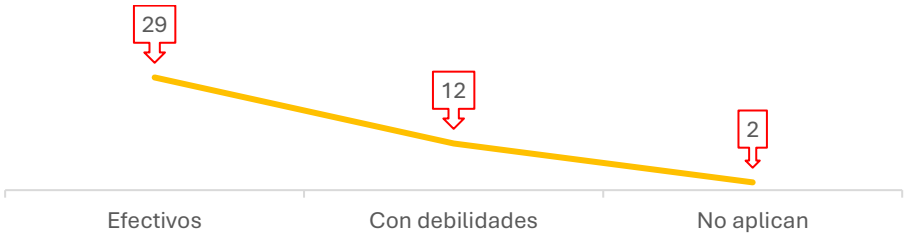
RIESGO #	PROCESO	CONTROL #	CONTROL	SOPORTE	SEGUIMIENTO OCI	CUMPLE
28	Gestión Estratégica del Talento Humano.	1	La Dirección de Gestión Humana define el acceso de los usuarios autorizados y el equipo de archivo de la DGH, controlará el acceso al repositorio de historias laborales para la consulta y manejo de esta documentación, en caso de que los usuarios no cuenten con la autorización de acceso, no se permitirá la consulta a dichos expedientes, como evidencia se tendrá la base de préstamos de historias laborales. el cargue de evidencia se realizará Semestralmente	Base de préstamos de historias laborales	Se evidencia la ejecución parcial de la base de Préstamo y consulta de Historias Laborales de los meses de enero, marzo y abril 2025.	SI
29	Gestión Financiera.	1	El responsable de las áreas que componen la dirección financiera (Presupuesto, Pago y contabilidad) informa al director financiero cada vez que se requiera las solicitudes respecto a los permisos de acceso y/o cancelación de usuarios al aplicativo donde se registra la información financiera, para que se realice la gestión ante la Dirección de tecnologías de la Información, en caso de que los usuarios no cuenten con la autorización de acceso, no se permitirá la consulta a dicha información, como evidencia se tendrá los comunicados oficiales y/o correo electrónicos de las solicitudes de acceso y/o cancelación de usuarios.	comunicado oficial y/o correo electrónico	Se evidencia la ejecución de la actividad mediante la presentación de dos formatos de solicitud de creación de usuarios, así como dos correos electrónicos relacionados con la desactivación de usuarios adscritos a la Dirección Financiera.	SI
30	Gestión Integral a las Personas Privadas de la Libertad - PPL.	1	El Secretario del Centro Especial de Reclusión, registra y valida cuando se requiera las solicitudes de acceso a información archivada, validando previamente que las mismas hayan sido autorizadas por la Dirección del C.E.R a través de memorando y/o correo electrónico; a su vez tendrá a su cargo las llaves del archivador de documentos ubicado en el área administrativa del Centro, en caso de no contar con solicitud o requerimiento previo se debe solicitar esta autorización a la dirección del CER, una vez sea autorizada, se debe dejar este soporte para efectos de trazabilidad, la evidencia se reportara de forma Cuatrimestral	memorando y/o correo electrónico	Se evidencia la ejecución de la actividad mediante el memorando en el que se socializan los lineamientos relacionados con el archivo de las hojas de vida jurídicas y de salud en el Centro Especial de Reclusión. En el cuerpo del correo que acompaña dicho memorando, también se abordan aspectos relacionados con la ubicación y el control de las llaves del archivo.	SI

RIESGO #	PROCESO	CONTROL #	CONTROL	SOPORTE	SEGUIMIENTO OCI	CUMPLE
31	Gestión Jurídica.	1	El responsable del equipo de archivo de la Dirección Jurídica y Contractual anualmente realiza la intervención documental de los expedientes en referencia a la completitud y correspondencia de archivos de los expedientes que se maneja en el área, como evidencia se genera el inventario documental de la DJC. En caso de no entregar el inventario documental a las instancias correspondientes se debe informar al Director(a) Jurídico(a) y Contractual de las acciones para dar cumplimiento.	Inventario Documental de la DJC	Se evidenció la ejecución de la actividad con el inventario documental de los meses de enero a abril. información de Archivo Contratos y Jurídica	SI
32	Gestión Tecnológica de Seguridad y Emergencias.	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.	Reporte mensual de mantenimiento	Se evidencia la ejecución parcial de la actividad, mediante la presentación de los informes mensuales de interventoría correspondientes a los meses de enero, febrero y marzo de 2025. Sin embargo, se encuentra pendiente la entrega del informe correspondiente al mes de abril, así como los reportes de seguimiento a los mantenimientos realizados durante el mismo período. **Recomendación:** Se recomienda consolidar y presentar la información pendiente para completar la trazabilidad del control establecido, asegurando la continuidad en el seguimiento y la documentación de las actividades ejecutadas.	NO
32	Gestión Tecnológica de Seguridad y Emergencias.	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.	Informe Mensual de Empresa Contratista	Se evidencia la ejecución mensual de los informes de mantenimiento correspondientes a los meses de enero, febrero y marzo de 2025. No obstante, se encuentra pendiente la presentación del informe correspondiente al mes de abril. **Recomendación:** Se sugiere realizar el seguimiento respectivo para garantizar la entrega oportuna del informe de abril, a fin de mantener la continuidad y trazabilidad del control establecido.	NO

RIESGO #	PROCESO	CONTROL #	CONTROL	SOPORTE	SEGUIMIENTO OCI	CUMPLE
33	Gestión y Análisis de la Información.	1	El Profesional Universitario, Especializado y/o Contratista de la Oficina de Análisis de Información y Estudios Estratégicos responsable de la bodega de datos valida mensualmente que la carga de información de las fuentes haya finalizado exitosamente por medio de consultas SQL en el rango de fechas actualizado; cuyo resultado es evidenciado en el indicador de gestión "cumplimiento en la actualización de la bodega de datos" el cual es reportado periódicamente en el Portal MIPG. En caso de incumplimiento de este indicador se deberá realizar la justificación pertinente en el Portal MIPG. Como evidencias se adjunta la consulta SQL y el cargue en el portal MIPG del indicador de gestión asociado.	Indicador de Gestión	La evidencia aportada no permite validar la ejecución de la actividad de control, ya que únicamente se presentaron los archivos en Excel correspondientes a la "Consulta Actualización Bodega" del primer cuatrimestre de 2025. Sin embargo, no se anexó la evidencia del indicador de gestión asociado, lo cual impide confirmar el cumplimiento efectivo de la actividad. **Recomendación:** Se sugiere complementar la información suministrada con el reporte o soporte del indicador de gestión correspondiente, debidamente actualizado y validado, que permita verificar el impacto y cumplimiento de la actividad de control ejecutada.	NO

Tabla N. 9. Seguimiento ejecución de controles Elaboración propia – Fuente: repositorio evidencias ejecución de controles asociados a riesgos de seguridad de la información administrada por la DTSI.

Durante el seguimiento a la implementación de los 43 controles establecidos, se evidenció que 29 resultaron efectivos, 12 presentaron debilidades, y los 2 restantes no aplican para el período evaluado debido a su periodicidad semestral. Frente a los controles con observaciones, se hace necesario atender las recomendaciones propuestas en la tabla anterior, con el fin de fortalecer su efectividad y mitigar posibles riesgos asociados, como se detalla:



Grafica N. 3 Resultados seguimiento ejecución de controles, Elaboración propia – Fuente: repositorio evidencias ejecución de controles asociados a riesgos de seguridad de la información administrada por la DTSI.

OBSERVACIÓN N. 3 DEBILIDADES FRENTE AL CUMPLIMIENTO DEL NUMERAL ETAPA 8. MONITOREO, REVISIÓN Y REPORTE DE LA GUIA DE ADMINISTRACIÓN DE LOS RIESGOS G-FI-04 V3.

Se identificaron debilidades en el cargue de evidencias de los controles para el 28% (12/43) los cuales se reportaron de manera incompleta, lo anterior, denota falencias frente al criterio dispuesto en el numeral 11.7 titulada *Etapa 8. Monitoreo, Revisión y Reporte de la Guía de Administración de los riesgos G-FI-04 V3 del Sistema Integrado de Gestión SIG*, ocasionando que se afecten los pilares de seguridad de la información (integridad, confidencialidad y disponibilidad).

Recomendación: Fortalecer la calidad de la evidencia que respalda la ejecución de los controles, garantizando trazabilidad y cumplimiento de los criterios establecidos, especialmente en cuanto a acciones correctivas ante desviaciones, lo anterior, complementando con un monitoreo riguroso por parte de la segunda línea de defensa.

5. CONCLUSIONES

- La entidad presenta avances en la identificación, implementación, monitoreo y seguimiento asociados a los riesgos de seguridad de la información, destacándose la articulación entre las líneas de defensa y el cumplimiento de la política institucional.

- Persisten oportunidades de mejora detectadas en el Informe de Seguimiento a los Riesgos de seguridad de la Información tercer cuatrimestre 2025, Radicado N. 3-2025-7706, como:

> ***"Oportunidad de Mejora N°1****: 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".*
>
> ***"Oportunidad de Mejora N°4:*** *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".*

- Por otra parte, se Identificó la falta de inclusión del proceso de Gestión de Conocimiento e Innovación Pública en los registros de activos, en concordancia con las tablas de retención documental, así como en atención a la Guía de Administración del Riesgo de la SDSCJ (G-FI-04 V3).

- También, se observó que actualmente la valoración de riesgos de seguridad de la información se basa en vulnerabilidades identificadas en lugar de amenazas, lo cual requiere validación y ajuste, toda vez que los resultados no son consistentes con el número de riesgos determinados por proceso y desatienden lo estipulado en el numeral 6.3 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6, emitida por el DAFP.

- Se identificaron brechas en la documentación y trazabilidad de algunas actividades de control, especialmente aquellas relacionadas con la respuesta ante desviaciones, así como debilidades en la evidencia de ejecución de controles.

6. RECOMENDACIONES

- Atender con prioridad las observaciones y oportunidades de mejora identificadas, estableciendo planes de mejora con responsables definidos, cronogramas y seguimiento periódico.

- Fortalecer la calidad de la evidencia que respalda la ejecución de los controles, garantizando trazabilidad y cumplimiento de los criterios establecidos, especialmente en

cuanto a acciones correctivas ante desviaciones, lo anterior, complementando con un monitoreo riguroso por parte de la segunda línea de defensa.

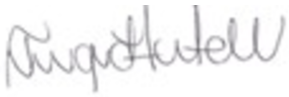
- Revisar y ajustar la metodología de valoración del riesgo, asegurando el enfoque en amenazas como lo establece la Guía de Administración de Riesgos del DAFP.

- Actualizar periódicamente la matriz de riesgos y activos de información, y su publicación versionada incorporando todos los procesos, a fin de garantizar una visión integral y actualizada del panorama de riesgos.

- Diferenciar las estrategias de tratamiento del riesgo residual de acuerdo con la criticidad e impacto de cada situación, incorporando análisis de costo-beneficio y criterios de aceptabilidad institucional.

- Consolidar la tipología de controles (manuales y automáticos) en la matriz institucional, promoviendo una visión integral del entorno de control y facilitando la evaluación de su eficiencia.

Elaboró:



Ingrid Beatriz Acosta Velasquez

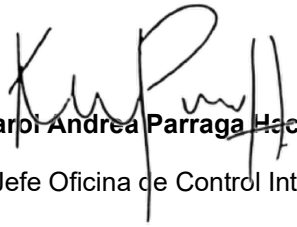
Contratista Oficina de Control Interno

Revisó:

Diego Alexander Urazán Franco

Contratista Oficina de Control Interno

Aprobó:



Karol Andrea Parraga Hache

Jefe Oficina de Control Interno