ALCALDÍA MAYOR DE BOGOTÁ
SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA
AL RESPONDER CITAR EL NR.
Nro. Rad: 3-2025-42443
Fecha: 24/10/2025 03:00:45 PM
Destino: 100-DESPACHO

MEMORANDO

Para: CESAR ANDRES RESTREPO FLOREZ DESPACHO SECRETARIO DE SEGURIDAD

De: OFICINA DE CONTROL INTERNO

Asunto: INFORME DE SEGUIMIENTO A CONTROLES ASOCIADOS A RIESGOS DE SEGURIDAD DE LA INFORMACIÓN CORRESPONDIENTE AL SEGUNDO 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 V3), la Oficina de Control Interno presenta el Informe de Seguimiento a los Controles asociados a los Riesgos de Seguridad de la Información, correspondiente al segundo cuatrimestre de 2025, en el cual, de manera general, se concluye lo siguiente:

- En relación con la consistencia metodológica en la identificación y valoración de riesgos, se evidenció que los riesgos están correctamente vinculados a activos específicos, con causas, amenazas y vulnerabilidades claramente diferenciadas, lo cual refleja una aplicación adecuada de la metodología definida en la Guía G-FI-04 V4 y la Política PO-FI-02 V3.

- Se observan avances en identificación y valoración de activos, toda vez que, se ha fortalecido la clasificación de activos según criterios de criticidad (confidencialidad, integridad y disponibilidad), aunque se mantiene pendiente la publicación de la versión actualizada de la matriz F-GD-1081.

- Se subsanó la oportunidad de mejora relacionada con la ausencia de riesgos y controles en el proceso de Gestión Documental, evidenciando capacidad de respuesta ante incidentes previos.

- Se evidencia un avance en la ejecución de controles y en la reducción de observaciones frente al primer cuatrimestre de 12 observaciones / 43 controles (28%) a 10 observaciones / 47 controles (21%), lo que refleja una mejora en la gestión documental y operativa de los riesgos de seguridad de la información.

- Persistencia de brechas en soportes documentales. A pesar de los avances, continúan observándose inconsistencias en el cargue de evidencias, especialmente en la etapa de monitoreo, revisión y reporte, lo cual limita la trazabilidad y verificación de la actividad de control.

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

- Los planes de mejora específicos (N.º 556, 557, 558), con fecha de cierre prevista para el 31 de diciembre de 2025, serán objeto de verificación para el tercer cuatrimestre 2025.

A partir de los resultados del seguimiento realizado, se deberá formular los planes de mejoramiento a que haya lugar por la Dirección de Gestión Humana 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 por parte del Líder del Proceso auditado será de ocho (8) días hábiles, contados a partir de la comunicación y/o notificación que generará el aplicativo de gestión y/o herramienta dispuesta.

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/transparencia/planeacion-presupuesto-ingresos/informes-control-interno

Cordialmente,

KAROL ANDREA PARRAGA HACHE
JEFE DE OFICINA CONTROL INTERNO

c.c.e.: IVAN HERSAYN PINILLA HERRERA-DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION
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 II 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 2025.

2. ALCANCE

El ejercicio de evaluación y seguimiento comprende el periodo entre el 01 de mayo al 31 de agosto de 2025, en referencia a la Matriz de Riesgos de Seguridad de la Información (F-FI-1385) vigente como las evidencias aportadas por los procesos.

Lo anterior, conforme al numeral 13, titulado PUBLICACIÓN, SEGUIMIENTO Y EVALUACIÓN A LOS RIESGOS, de la Política de Administración de Riesgos PO-FI-02 V2, el cual establece que la Primera Línea de Defensa es responsable de cargar los soportes documentales que evidencien la implementación de los controles, mientras que la Segunda Línea de Defensa debe realizar el seguimiento cuatrimestral a la Matriz de Riesgos y remitir el informe de resultados 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 V4).
- Política de Administración de Riesgos de la SDSCJ (PO-FI-02 V3).
- Política de Seguridad y Privacidad Información de la SDSCJ (PO-GT-1 V7).
- Matriz de Riesgos de Seguridad de la Información de la Entidad (F-FI-1385 V1).

4. SEGUIMIENTO DE AUDITORIA

4.1 CUMPLIMIENTO POLÍTICA ADMINISTRACIÓN DE RIESGOS.

La Secretaría Distrital de Seguridad, Convivencia y Justicia (SDSCJ) cuenta con documentos internos que se emplean como instrumentos metodológicos para la gestión de riesgos en materia de seguridad de la información. Entre ellos se destacan la Política de Administración de Riesgos y la Guía de Administración de Riesgos, esta última con especial énfasis en el acápite N.11, titulado "Identificación y Gestión del Riesgo (Riesgo Seguridad de la Información)". Ambos instrumentos fortalecen la prevención, promueven la integridad pública y consolidan la seguridad de la información, al orientar la identificación, análisis, valoración, tratamiento y monitoreo de riesgos mediante una metodología estructurada que define etapas clave para su implementación efectiva.

Lo anterior contribuye al cumplimiento de los objetivos estratégicos institucionales, en articulación con el Marco Integrado de Planeación y Gestión (MIPG), y facilita la toma de decisiones informadas en materia de riesgos de seguridad de la información. 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 martes 26 de agosto 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 26/08/2025. Fuente: Informe Segundo Cuatrimestre Riesgos de Seguridad de la Información - 2025 generado por la DTSI con radicado número 3-2025-36876

Se constató que la Dirección de Tecnologías y Sistemas de la Información (DTSI) emitió el memorando electrónico N. 3-2025-31544, con fecha del 8 de agosto de 2025, en el cual se establecen los lineamientos para el cargue de evidencias relacionadas con los controles implementados para la mitigación de riesgos de seguridad de la información, correspondientes al segundo cuatrimestre (mayo a agosto) de la vigencia 2025, dirigidas a los procesos definidos en la Matriz de Riesgos de la Secretaría.

Asimismo, se observó la realización de la difusión institucional mediante comunicación enviada por correo electrónico el día 29 de agosto de 2025, a las áreas responsables, en la cual se brindaron orientaciones específicas para el cargue de evidencias y se impartieron instrucciones sobre la validación de las observaciones formuladas por la Oficina de Control Interno durante la vigencia 2025, con el fin de fortalecer las actividades de seguimiento.

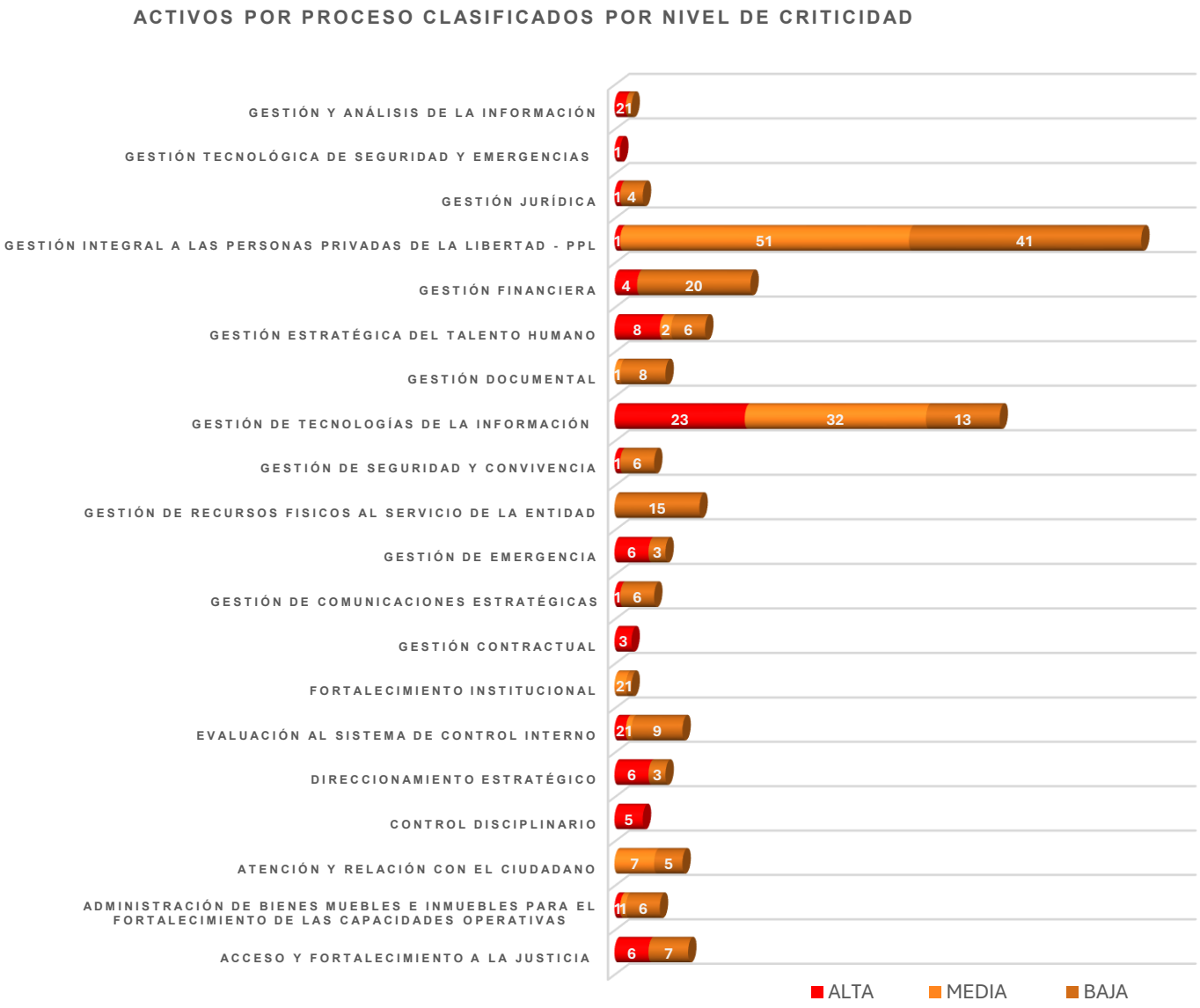
4.1.2 ETAPA 2: IDENTIFICACIÓN DE ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN

En concordancia con el Informe de Riesgos de Seguridad de la Información correspondiente al segundo cuatrimestre de 2025, emitido por la Dirección de Tecnologías y Sistemas de la Información (DTSI) mediante radicado N. 3-2025-36876 del 12/09/2025, y en verificación de la información aportada por el proceso, se evidenció la realización de mesas de trabajo entre el personal de la Dirección de Recursos Físicos y Gestión Documental y la DTSI, orientadas a la actualización de activos de información en la matriz F-GD-1081 (Registro de Activos de Información e Índice de Información Clasificada y Reservada). El proceso reporta que dicha matriz será publicada en el sitio web institucional al cierre de la vigencia 2025, junto con la actualización integral de los activos de información correspondientes a los procesos de la Entidad.

No obstante, durante la revisión de la matriz F-GD-1081 V2, se determinó que, si bien se evidencian avances en la identificación de nuevos activos de información, la versión oficial publicada continúa siendo la versión 2. Sobre dicha versión, la Oficina de Control Interno realizó el seguimiento a la adecuada identificación de los activos de información registrados en la Secretaría de Seguridad, Convivencia y Justicia – SDSCJ.

Actualmente, la matriz registra un total de 322 activos de información asociados a 20 procesos institucionales, clasificados según su nivel de criticidad en: 71 activos de criticidad alta, 154 de criticidad media y 97 de criticidad baja. Esta clasificación se evaluó con base en los tres principios fundamentales de la seguridad de la información: Confidencialidad, Integridad y Disponibilidad.

La distribución por proceso, según el nivel de criticidad de los activos, se detalla a continuación:



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

Se observó que persiste la **Oportunidad de Mejora 1**. registrada en el Informe de Seguimiento a los Riesgos de Seguridad de la Información I Cuatrimestre de 2025 con Radicado N. 3-2025-24957 del 27 de junio de 2025, que señala "*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*". De lo anterior, aunque no constituye un incumplimiento, representa una desatención a la recomendación de la Oficina de Control Interno, que está orientada a promover la adopción de mejores prácticas institucionales, la consolidación de evidencias verificables y la alineación con los principios de acceso a la información. Se reitera la importancia de publicar la

versión actualizada de la matriz, conforme a los ajustes realizados, ya sea por disposiciones normativas o por cambios derivados en el contexto interno.

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

Se evidenció que el registro de activos F-GD-1081 cumple con la incorporación de los ocho (8) criterios establecidos en el numeral 12.2.1 "*Etapa 3: pasos para la identificación y/o valoración de activos) de la Guía de administración de riesgos G-FI-04 V.4*", tales como: Información del proceso, tipo documental, tipo de soporte, clasificación documental, clasificación y custodia de información, Índice de Información clasificada y reservada, infraestructura crítica cibernética y componentes de seguridad de la información.

En relación al criterio N. 8. "Componente de Seguridad de la Información", en donde se imparten lineamientos para evaluar la criticidad de los activos, clasificando el grado de importancia de cada Activo de información de acuerdo con la Confidencialidad, Integridad y Disponibilidad (Alta, Media y Baja), y de acuerdo con lo definido en el Anexo 4 "lineamientos para la gestión de riesgos de seguridad digital en Entidades públicas" del MinTIC. Se efectuó validación respecto a su adecuada clasificación teniendo en cuenta la tabla de valoración de la Guía para la administración del riesgo G-FI-04_V4:

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o más componentes (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta o media en al menos uno (1) de sus componentes
BAJA	Activos de información en los cuales la clasificación de la información en todos sus componentes es baja.

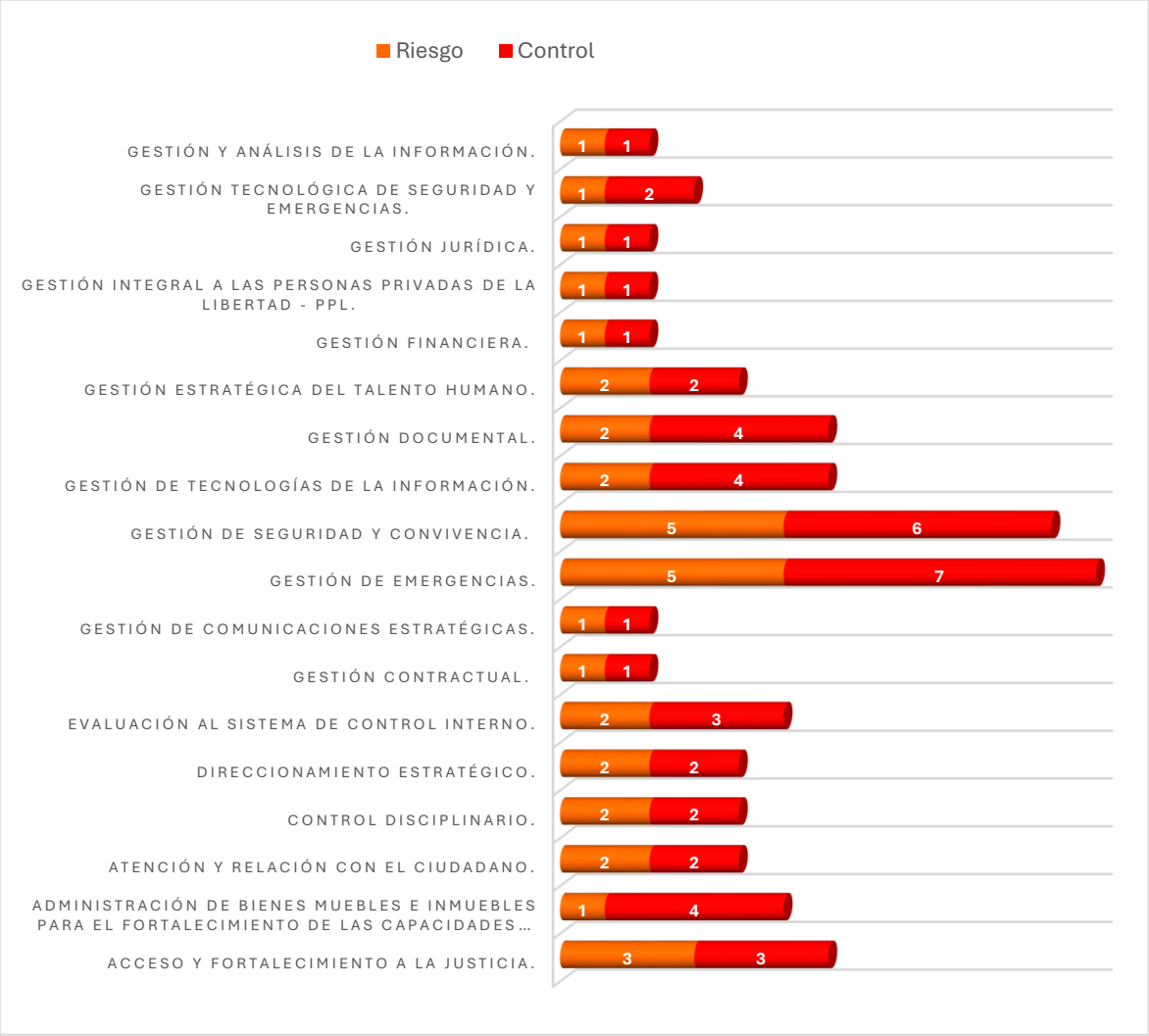
Imagen 2. Tabla de valoración. Fuente: Guía para la administración del riesgo G-FI-04_V4.

La revisión permitió verificar que la categorización asignada por la segunda línea guarda coherencia con los niveles de impacto potencial sobre la confidencialidad, integridad y disponibilidad de la información, contribuyendo así al fortalecimiento del análisis de riesgos y a la adecuada priorización de medidas de protección.

De otra parte, se identifica que, pese al desarrollo de mesas de trabajo con el proceso de Gestión de Conocimiento e Innovación Pública para atender la "***OBSERVACION 1: FALTA DE INCLUSIÓN DEL PROCESO DE GESTIÓN DEL CONOCIMIENTO EN EL REGISTRO DE ACTIVOS DE INFORMACIÓN"***, previamente señalada en el Informe de Seguimiento a los Riesgos de Seguridad de la Información I Cuatrimestre de 2025 con Radicado N. 3-2025-24957 del 27 de junio de 2025, Se observó que, la versión actual del documento F-GD-1081 V1 continúa sin contemplarlo. No obstante, se constató que la inconsistencia detectada está siendo abordada mediante la acción definida en el **plan de mejora N. 556**, actualmente en términos de ejecución, cuya fecha de finalización está prevista para el 31 de diciembre de 2025.

4.1.4 ETAPA 4: IDENTIFICACIÓN DEL RIESGO:

Resultado del análisis de la matriz de riesgos de seguridad de la información de la entidad (F-FI-1385), Se identificó un total de 35 riesgos y 47 controles asociados para su mitigación, con una distribución específica por cada proceso, como se detalla:



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 - II Cuatrimestre 2025

Se identificó que la Matriz de Riesgos de Seguridad de la Información de la Entidad (F-FI-1385) cumple con los criterios mínimos establecidos para la clasificación de riesgos asociados a la pérdida de confidencialidad, integridad o disponibilidad. Cada riesgo está vinculado a un activo específico dentro de su respectivo proceso, y se relacionan de manera estructurada las amenazas y vulnerabilidades que podrían generar su materialización. Asimismo, se constató que las causas mitigadas corresponden a vulnerabilidades previamente documentadas, en concordancia con lo establecido en la Guía para la Administración de los Riesgos V6 y alineado

con la metodología definida en la Política de Administración de Riesgos de la Entidad (PO-FI-02 V3). A continuación, se presentan algunos ejemplos seleccionados aleatoriamente de la matriz (F-FI-1385) que sustentan la adecuada estructura:

RIESGO #	PROCESO	ACTIVO	CAUSA MITIGADA	RIESGO	AMENAZA	VULNERABILIDAD	CONSECUENCIA
1	Acceso y Fortalecimiento a la Justicia.	✓Registros DAJ (Registros de orientaciones y atenciones en Centros de Recepción e Información de Casas de Justicia, Registros de orientaciones y atenciones en Unidades Móviles de Acceso a la Justicia, Registros de orientaciones en canales no presenciales de Casas de Justicia, Registros de orientaciones y atenciones en Unidades de Mediación y Conciliación, Registros de orientaciones de la estrategia de facilitadores de acceso a la justicia)	✓Asignación errada de los derechos de acceso.	✓Pérdida de la Integridad	✓Abuso de derechos.	✓Asignación errada de los derechos de acceso.	Pérdida o detrimento de información
2	Acceso y Fortalecimiento a la Justicia.	✓Formularios (Formulario de forms registro atenciones virtuales Centro de Recepción e Información CRI, Formulario de forms registro jornadas unidades móviles para el acceso a la justicia, Formulario forms encuesta de satisfacción Dirección de Acceso a la Justicia)	✓Asignación errada de los derechos de acceso.	✓Pérdida de la Confidencialidad	✓Abuso de derechos.	✓Asignación errada de los derechos de acceso.	Pérdida o detrimento de información
3	Acceso y Fortalecimiento a la Justicia.	✓Bases de datos información operativa de los programas y estrategias DRPA	✓Ausencia de copias de respaldo.	✓Pérdida de la Integridad	✓Error en el uso	✓Ausencia de copias de respaldo.	Pérdida o detrimento de información
4	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	✓Base de datos del Sistema de información y administración de Bienes SIMBA	✓Asignación errada de los derechos de acceso.	✓Pérdida de la Integridad	✓Error en el uso	✓Asignación errada de los derechos de acceso. Ausencia de copias de respaldo. Falla en la producción de informes de gestión. Gestión deficiente de las contraseñas.	Interrupción de los sistemas / procesos
19	Gestión de Emergencias.	✓Bitácora de transferencia de mando área de seguimiento	✓Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad.	✓Pérdida de la Disponibilidad	✓Saturación del sistema de información.	✓Ausencia de planes de continuidad.	Reclamaciones o quejas de ciudadanos
20	Gestión de Seguridad y Convivencia.	✓Registro Documental SSC (Registros y evidencias de actividades gestionadas para lograr el control, la prevención del delito y promover la convivencia pacífica.)	✓Ausencia del personal.	✓Pérdida de la Integridad y Disponibilidad	A✓buso de derechos.	✓Falta de control periódico sobre los derechos de acceso. Ausencia de guías para el adecuado uso de la plataforma	Pérdida o detrimento de información Demoras en los servicios prestados y ejecución de los procesos
21	Gestión de Seguridad y Convivencia.	✓Reportes de Seguridad Ciudadana	✓Gestión deficiente de las contraseñas.	✓Pérdida de la Confidencialidad	✓Abuso de Derechos Corrupción de Datos Error en el uso	✓Acceso y uso inadecuado de la información	Pérdida o detrimento de información Pérdida de confianza del ciudadano Demandas, litigios, derechos de petición o tutelas
22	Gestión de Seguridad y Convivencia.	✓Actas de Concejos Locales de Seguridad.	✓Respuesta inadecuada de mantenimiento del servicio.	✓Pérdida de la Disponibilidad	✓Gestión Inadecuada de la Información	✓Acceso y uso inadecuado de la información	Pérdida o detrimento de información Pérdida de confianza del ciudadano Demandas, litigios, derechos de petición o tutelas

Tabla N.1 Elaboración Oficina de Control Interno. Fuente: Matriz de riesgos de seguridad de la información F-FI-1385 - II Cuatrimestre 2025

La adecuada identificación de los riesgos de seguridad de la información en la Secretaría de Seguridad, Convivencia y Justicia (SDSCJ), constituye un insumo base para la transición hacia La Guía para la Gestión Integral del Riesgo Versión 7, la cual incorpora nuevos enfoques en materia de apetito, tolerancia y capacidad de riesgo, así como una gestión más integral de los riesgos tecnológicos y de ciberseguridad.

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 primer 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) **Según** radicado número 3-2025-36876 del 12/09/2025	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.	En atención a la observación sobre la falta de inclusión de riesgos y controles de seguridad de la información asociados al proceso de Gestión Documental, se informa que se llevaron a cabo mesas de trabajo de actualización de activos de información, en las cuales se adelantó la identificación, análisis y documentación de riesgos y controles correspondientes a los activos de información calificados con criticidad alta, de acuerdo con los lineamientos definidos en la Política de Administración de Riesgos de la Entidad. Los riesgos y controles identificados son incorporados en la Matriz de Riesgos de Seguridad de la Información, la cual es publicada en el sitio web institucional una vez consolidada, garantizando visibilidad, trazabilidad y transparencia en la gestión. **Documentación Mesas de Trabajo:** Las mesas de trabajo y actividades llevadas a cabo por la Dirección de Recursos Físicos y Gestión Documental y la Dirección de Tecnologías y Sistemas de la Información, sobre la actualización de activos de información y la creación de controles y riesgos de seguridad de la Información, para la atención de la oportunidad de Mejora 1 (Primer Cuatrimestre), así: ❖ Acta Actualización Activos de Información Proceso Gestión Documental. ❖ Acta Riesgos de seguridad Información Proceso Gestión Documental. ❖ Matriz de Riesgos de seguridad Información Proceso Gestión Documental.	**Resultado:** Se observa la ejecución de la acción de mejora con la inclusión de riesgos y controles asociados al proceso de gestión documental, verificado en la Matriz de Riesgos de seguridad Información (F-FI-1385) Por lo anterior, **Se subsana la oportunidad de mejora N.1**

Tabla N. 2. Gestión Adelantada frente a las Oportunidades de Mejora emitidas por OCI – Etapa 4. Fuente: Informe Segundo Cuatrimestre Riesgos de Seguridad de la Información - 2025 generado por la DTSI con radicado número 3-2025-36876 del 12/09/2025

Como resultado del seguimiento realizado a la oportunidad N°1, previamente registrada como pendiente de ejecución en el Informe de Seguimiento a los Riesgos de Seguridad de la Información I Cuatrimestre de 2025 con Radicado N. 3-2025-24957 del 27 de junio de 2025, esta Oficina valida la realización de la actividad correspondiente, sustentada mediante los soportes documentales aportados por el proceso en el Informe Segundo Cuatrimestre Riesgos de Seguridad de la Información - 2025 generado por la DTSI con radicado número 3-2025-36876 del 12 de septiembre de 2025.

4.1.5 ETAPA 5: VALORACIÓN DEL RIESGO

En relación con la valoración del riesgo inherente con base en las amenazas, esta oficina fundamentó su evaluación conforme a lo establecido en el numeral 6.3 “Valoración del riesgo” de la Guía para la Administración de los Riesgos V6:

RIESGO	ACTIVO	AMENAZA	VULNERABILI-DAD	PROBABILIDAD	IMPACTO	ZONA DE RIESGO
Pérdida de la Confiden-cialidad	Base de datos de nómina	Modificación no autorizada	Ausencia de políticas de control de acceso	4-Probable	4- Mayor	Extrema
			Contraseñas sin protección			
			Ausencia de mecanismos de identificación y autenticación de usuarios			
			Ausencia de bloqueo de sesión			

Una (1) sola valoración de Riesgo con base en las amenazas no en las vulnerabilidades.

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

Imagen. 3. Fuente: Numeral 6.3 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6.

Imagen. 4. Fuente: Numeral 6.3 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6.

Se observó que la Dirección de Tecnologías y Sistemas de la Información (DTSI) adelantó actividades orientadas a subsanar la causa que originó la ***OBSERVACIÓN N.2 INCONSISTENCIAS EN LA VALORACIÓN DE LA PROBABILIDAD O IMPACTO CON BASE EN LAS VULNERABILIDADES***, señalada en el Informe de Seguimiento a los Riesgos de Seguridad de la Información – I Cuatrimestre de 2025 (Radicado N.º 3-2025-24957 del 27 de junio de 2025). Como resultado, se verificó que, para cada riesgo de seguridad de la información, la DTSI determinó un único riesgo inherente, sustentado en la valoración de la probabilidad e impacto con base en las amenazas identificadas y no en las vulnerabilidades, conforme a lo establecido en la Guía para la Administración de los Riesgos. Lo anterior constituye un avance técnico que permitirá efectuar el cierre del **Plan de Mejora N.º 557**, derivado de dicha observación, cuya fecha de finalización está prevista para el 31 de diciembre de 2025. No obstante, el plan aún se encuentra en estado abierto y será objeto de seguimiento posterior por parte de la Oficina de Control Interno para validar la efectividad de dicho plan.

A continuación, se presenta la valoración de los 35 riesgos, cada uno con su respectiva evaluación de probabilidad e impacto, determinada con base en las amenazas identificadas. Esta valoración incluye el nivel de riesgo inherente resultante y se encuentra alineada con el mapa de calor establecido en la Política de Administración de Riesgos de la SDSCJ (PO-FI-02 V3):

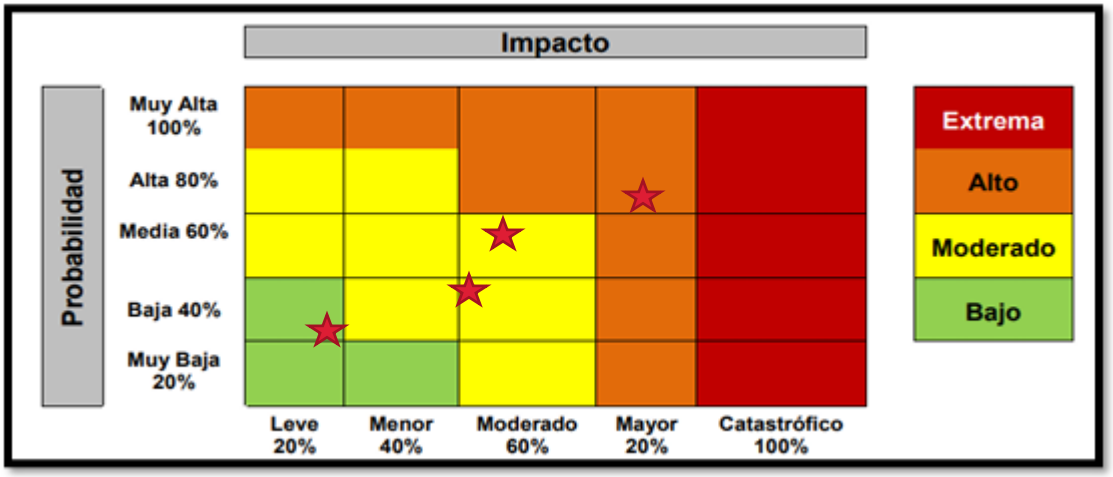


Imagen 5. Fuente: Política de Administración de Riesgos SDSCJ (PO-FI-02 V3).

Resultados consolidados por proceso:

RIESGO #	PROCESO	RIESGO	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO INHERENTE
1	Acceso y Fortalecimiento a la Justicia.	Pérdida de la Integridad	Abuso de derechos.	Baja	Moderado	MODERADO ✓
2	Acceso y Fortalecimiento a la Justicia.	Pérdida de la Confidencialidad	Abuso de derechos.	Baja	Moderado	MODERADO ✓
3	Acceso y Fortalecimiento a la Justicia.	Pérdida de la Integridad	Error en el uso	Baja	Leve	BAJA ✓
4	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	Pérdida de la Integridad	Error en el uso	Media	Leve	MODERADO ✓
5	Atención y Relación con el Ciudadano.	Pérdida de la Integridad Pérdida de Confidencialidad	Error en el uso	Media	Leve	MODERADO ✓
6	Atención y Relación con el Ciudadano.	Pérdida de la Integridad Pérdida de Confidencialidad	Divulgación	Muy Baja	Moderado	MODERADO ✓
7	Control Disciplinario.	Pérdida de la Integridad	Corrupción de los datos	Baja	Moderado	MODERADO ✓
8	Control Disciplinario.	Pérdida de la Confidencialidad	Abuso de derechos.	Baja	Moderado	MODERADO ✓
9	Direccionamiento Estratégico.	Pérdida de la Disponibilidad	Incumplimiento de la Divulgación	Baja	Mayor	ALTO ✓
10	Direccionamiento Estratégico.	Pérdida de la Confidencialidad	Divulgación	Muy Baja	Moderado	MODERADO ✓

RIESGO #	PROCESO	RIESGO	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO INHERENTE
11	Evaluación al Sistema de Control Interno.	Pérdida de la Integridad	Corrupción de datos. Indisponibilidad del sistema de información Mal funcionamiento del software.	**Baja**	**Moderado**	**MODERADO** ✓
12	Evaluación al Sistema de Control Interno.	Pérdida de la Integridad	Corrupción de datos. Indisponibilidad del sistema de información Mal funcionamiento del software.	**Baja**	**Moderado**	**MODERADO** ✓
13	Gestión Contractual.	Pérdida de la Disponibilidad Pérdida de la Integridad	Corrupción de los datos Fenómenos Ambiental Pérdida de Información"	**Baja**	**Moderado**	**MODERADO** ✓
14	Gestión de Comunicaciones Estratégicas.	Pérdida de la Confidencialidad y Pérdida de la Integridad	Divulgación Actividad Maliciosa de Ciberdelincuente Datos provenientes de fuentes no confiables	**Muy Baja**	**Moderado**	**MODERADO** ✓
15	Gestión de Emergencias.	Pérdida de la Confidencialidad	Fallas del equipo.	**Baja**	**Moderado**	**MODERADO** ✓
16	Gestión de Emergencias.	Pérdida de la Disponibilidad	Mantenimiento de equipos Inadecuado	**Baja**	**Moderado**	**MODERADO** ✓
17	Gestión de Emergencias.	Pérdida de Confidencialidad, Integridad y/o disponibilidad de la información	Falla en equipo de telecomunicaciones	**Muy Baja**	**Moderado**	**MODERADO** ✓
18	Gestión de Emergencias.	Pérdida de la Disponibilidad	Saturación del sistema de información.	**Media**	**Menor**	**MODERADO** ✓
19	Gestión de Emergencias.	Pérdida de la Disponibilidad	Saturación del sistema de información.	**Baja**	**Menor**	**MODERADO** ✓
20	Gestión de Seguridad y Convivencia.	Pérdida de la Integridad y Disponibilidad	Abuso de derechos.	**Muy Baja**	**Moderado**	**MODERADO** ✓
21	Gestión de Seguridad y Convivencia.	Pérdida de la Confidencialidad	Abuso de Derechos Corrupción de Datos Error en el uso	**Baja**	**Moderado**	**MODERADO** ✓
22	Gestión de Seguridad y Convivencia.	Pérdida de la Disponibilidad	Gestión Inadecuada de la Información	**Baja**	**Moderado**	**MODERADO** ✓
23	Gestión de Seguridad y Convivencia.	Pérdida de la Confidencialidad	Abuso de derechos. Datos provenientes de fuentes no confiables Error en el uso	**Baja**	**Moderado**	**MODERADO** ✓
24	Gestión de Seguridad y Convivencia.	Pérdida de la Integridad	Abuso de derechos. Datos provenientes de fuentes no confiables Error en el uso	**Baja**	**Moderado**	**MODERADO** ✓
25	Gestión de Tecnologías de la Información.	Pérdida de Confidencialidad, integridad y/o disponibilidad de la información	Ciberataque Modificación de bases de datos	**Media**	**Mayor**	**ALTO** ✓
26	Gestión de Tecnologías de la Información.	Pérdida de Confidencialidad, integridad y/o disponibilidad de la información	"Uso no autorizado de credenciales de administración a cualquiera de los componentes de la infraestructura de la SDSCJ	**Baja**	**Mayor**	**ALTO** ✓

RIESGO #	PROCESO	RIESGO	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO INHERENTE
			Ciberataque o incidente informático a la infraestructura del proveedor de nube de la Entidad"…			
27	Gestión Documental.	Pérdida de la Disponibilidad	Error en el uso Fuego Inundación	**Muy Baja**	**Menor**	**BAJA** ✓
28	Gestión Documental.	Pérdida de la Confidencialidad Pérdida de la Integridad	Uso no autorizado del equipo o software.	**Baja**	**Moderado**	**MODERADO** ✓
29	Gestión Estratégica del Talento Humano.	Pérdida de la Integridad	Uso no autorizado del equipo o software.	**Baja**	**Moderado**	**MODERADO** ✓
30	Gestión Estratégica del Talento Humano.	Pérdida de la Confidencialidad	Abuso de derechos y corrupción de los datos	**Baja**	**Moderado**	**MODERADO** ✓
31	Gestión Financiera.	Pérdida de la Integridad	Corrupción de los datos	**Baja**	**Menor**	**MODERADO** ✓
32	Gestión Integral a las Personas Privadas de la Libertad - PPL.	Pérdida de la Disponibilidad Pérdida de Confidencialidad	Divulgación	**Baja**	**Moderado**	**MODERADO** ✓
33	Gestión Jurídica.	Pérdida de la Disponibilidad Pérdida de la Confidencialidad Pérdida de la Integridad	Corrupción de los datos Fenómenos Ambiental Pérdida de Información	**Baja**	**Moderado**	**MODERADO** ✓
34	Gestión Tecnológica de Seguridad y Emergencias.	Pérdida de Confidencialidad, Integridad y/o disponibilidad de la información	Falla en equipo de telecomunicaciones	**Baja**	**Moderado**	**MODERADO** ✓
35	Gestión y Análisis de la Información.	Pérdida de la Integridad	Error en el uso	**Baja**	**Mayor**	**ALTO** ✓

Tabla N. 3. Valoración de riesgos general por procesos. Elaboración OCI-Fuente: matriz de riesgos de seguridad de la información F-FI-1385

Derivado del análisis de probabilidad e impacto aplicado a cada proceso, se estableció la zona de riesgo inherente correspondiente, obteniendo un total de 35 valoraciones coherentes con los 35 riesgos identificados: cuatro (4) riesgos en nivel alto, veintinueve (29) en nivel moderado y dos (2) en nivel bajo, según se detalla a continuación:

, 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**	**1**	**0**	**1**
Atención y Relación con el Ciudadano.	**0**	**2**	**0**	**2**
Control Disciplinario.	**0**	**2**	**0**	**2**
Direccionamiento Estratégico.	**1**	**1**	**0**	**2**
Evaluación al Sistema de Control Interno.	**0**	**2**	**0**	**2**
Gestión Contractual.	**0**	**1**	**0**	**1**
Gestión de Comunicaciones Estratégicas.	**0**	**1**	**0**	**1**
Gestión de Emergencias.	**0**	**5**	**0**	**5**
Gestión de Seguridad y Convivencia.	**0**	**5**	**0**	**5**
Gestión de Tecnologías de la Información.	**2**	**0**	**0**	**2**

, PROCESO	ALTO	MODERADO	BAJO	TOTAL
Gestión Documental	0	1	1	2
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	1	0	1
Gestión y Análisis de la Información.	1	0	0	1
TOTAL	**4**	**29**	**2**	**35**

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

4.1.6 ETAPA 6: CREACIÓN DE CONTROLES:

Se presenta el consolidado de riesgos y controles identificados en cada proceso evaluado, en total, se registran treinta y cinco (35) riesgos y cuarenta y tres (43) controles, los cuales fueron clasificados y asociados conforme a su naturaleza, nivel de impacto y capacidad de mitigación. Esta información constituye la base para el análisis posterior de zonas de riesgo residual y efectividad de controles.

PROCESO	N. RIESGOS	N. CONTROLES
Acceso y Fortalecimiento a la Justicia.	3	3
Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	1	4
Atención y Relación con el Ciudadano.	2	2
Control Disciplinario.	2	2
Direccionamiento Estratégico.	2	2
Evaluación al Sistema de Control Interno.	2	3
Gestión Contractual.	1	1
Gestión de Comunicaciones Estratégicas.	1	1
Gestión de Emergencias.	5	7
Gestión de Seguridad y Convivencia.	5	6
Gestión de Tecnologías de la Información.	2	4
Gestión Documental	2	4
Gestión Estratégica del Talento Humano.	2	2
Gestión Financiera.	1	1
Gestión Integral a las Personas Privadas de la Libertad – PPL.	1	1
Gestión Jurídica.	1	1
Gestión Tecnológica de Seguridad y Emergencias.	1	2
Gestión y Análisis de la Información.	1	1
TOTAL	**35**	**47**

Tabla 5. Elaboración OCI-Fuente: matriz de riesgos de seguridad de la información F-FI-1385

Del análisis efectuado se observó que los (43) 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:

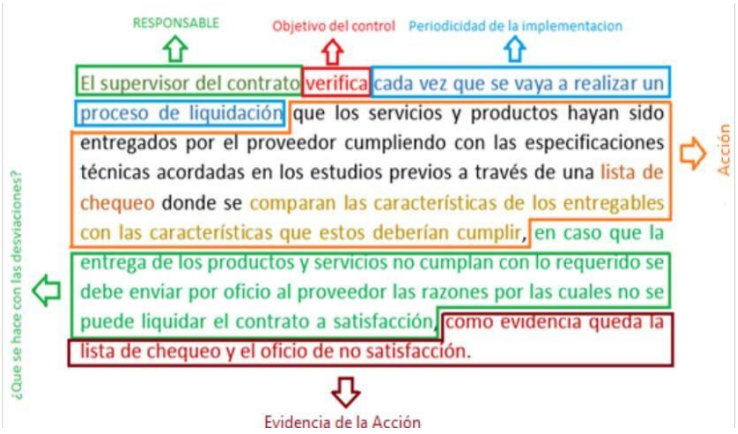


Imagen N. 6. Estructura Construcción Control. Fuente: numeral 9.7.1 de la Guía de administración de riesgos

La descripción de todos los controles cumple 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).

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 del 26/02/2025 en la etapa de creación de controles, se obtuvo el siguiente resultado:

OPORTUNIDAD DE MEJORA	REPORTE DE LA SEGUNDA LÍNEA DE DEFENSA (DTI) según radicado número 3-2025-36876 del 12/09/2025	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.	En atención a la oportunidad de mejora sobre la falta de inclusión de tipologías de controles automáticos y manuales en la estructuración de la Matriz de Riesgos de Seguridad de la Información, se informa que se adelantaron acciones orientadas a fortalecer las recomendaciones establecidas por la Oficina Control Interno así: Se realizó la revisión de los riesgos existentes en la matriz de riesgos de seguridad de la información, con el fin de validar valoración de la probabilidad o impacto con base en las vulnerabilidades de los siguientes procesos: ❖ Administración De Bienes Muebles E Inmuebles Para El Fortalecimiento De Las Capacidades Operativas (AB). ❖ Gestión Emergencias (GE). ❖ Gestión Tecnológica de Seguridad y Emergencias (GST). ❖ Gestión de Seguridad y Convivencia (GS). ❖ Gestión de Tecnología de Información (GT). Se realizó la revisión y validación de los controles establecidos en la matriz de riesgos de seguridad de la información, con el fin ajustar y garantizar su adecuada correspondencia frente a los riesgos identificados. así:	**Resultado:** Se evidencia que las acciones adelantadas por el proceso no subsanan la condición previamente detectada, respecto a la inclusión de tipologías de controles automáticos y manuales dentro de la matriz de riesgos de seguridad de la información. Esta falencia fue identificada en el Informe de Seguimiento a los Riesgos de Seguridad de la Información – Tercer Cuatrimestre de 2024, radicado N. 3-2025-7706, y persiste a pesar de la recomendación emitida en el Informe de Seguimiento a los Riesgos de Seguridad de la Información – Primer Cuatrimestre de 2025, radicado N. 3-2025-24957 del 27 de junio de 2025. Dado que esta situación fue objeto de revisión en el presente informe y no se evidencia su subsanación, se constituye como observación formal para la formulación del correspondiente plan de mejora

OPORTUNIDAD DE MEJORA	REPORTE DE LA SEGUNDA LÍNEA DE DEFENSA (DTI) según radicado número 3-2025-36876 del 12/09/2025	SEGUIMIENTO TERCERA LÍNEA DE DEFENSA (OFICINA DE CONTROL INTERNO)
	❖ Administración De Bienes Muebles E Inmuebles Para El Fortalecimiento De Las Capacidades Operativas (AB). ❖ Gestión Tecnológica de Seguridad y Emergencias (GST). ❖ Gestión Integral a las Personas Privadas de la Libertad - PPL. ❖ Oficina del Despacho. Adicionalmente, se incorporaron 2 riesgos y 4 controles adicionales, reforzando la cobertura y efectividad de la matriz de riesgos de seguridad de la Información, así: ❖ Gestión Documental (GD). De igual manera, se efectuó seguimiento al cargue de evidencias de controles de seguridad de la información, asegurando la validación de su implementación y el cumplimiento de los lineamientos establecidos para la mejora continua.	

Tabla N. 6. 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

OBSERVACIÓN N° 1 FALTA DE INCLUSIÓN DE TIPOLOGÍAS DE CONTROLES AUTOMÁTICOS Y MANUALES EN LA MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACION INSTITUCIONAL.

La matriz de riesgos de seguridad de la información F-FI-1385, para los controles identificados no contiene las tipologías (manuales y automáticos), descritos en el numeral 3.2.2.2 Tipología de controles y los procesos y 3.2.2.3 Análisis y evaluación de los controles– Atributos de la Guía para la administración de los riesgos V6 del DAFP y los numerales 11.7 y 11.7.2 de la Guía de administración de riesgos G-FI-04 V.4 de la Secretaría de Seguridad y Convivencia - SDSCJ. Esta situación se origina porque la matriz de riesgos de seguridad de la información (F-FI-1385) no contempla un campo específico para registrar dicha información, lo que ha limitado su documentación y actualización. Como consecuencia, se dificulta la evaluación integral de la efectividad y suficiencia de los controles, particularmente en lo relacionado con su automatización y dependencia tecnológica, lo anterior, podría generar inconsistencias en la evaluación del riesgo residual, afectando la precisión del mapa de riesgos y dificultando la priorización de acciones de mitigación.

RECOMENDACIÓN:

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.

Réplica del Proceso Auditado:

"En referencia al correo que antecede de forma respetuosa, nos permitimos realizar aclaración al Informe Preliminar Seguimiento a los Riesgos de Seguridad de la Información II Cuatrimestre 2025.

1. *En referencia a las consideraciones establecidas sobre la oportunidad de mejora N° 4 del informe de seguimiento a los riesgos de seguridad de la información primer cuatrimestre 2025 radicado mediante Memorando 3-2025-24957, así:*

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.

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 FFI-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.

Tomando como referencia las recomendaciones emitidas por la Oficina de Control Interno, se dio cumplimiento a través de las siguientes acciones, así:

- *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 FFI-1385 y clasificarlos según su tipología (automáticos o manuales).*

Se realizó la revisión de los riesgos existentes en la matriz de riesgos de seguridad de la información, con el fin de validar valoración de la probabilidad o impacto con base en las vulnerabilidades de los siguientes procesos:

- ❖ *Administración De Bienes Muebles E Inmuebles Para El Fortalecimiento De Las Capacidades Operativas (AB).*
- ❖ *Gestión Emergencias (GE).*
- ❖ *Gestión Tecnológica de Seguridad y Emergencias (GST).*
- ❖ *Gestión de Seguridad y Convivencia (GS).*
- ❖ *Gestión de Tecnología de Información (GT).*

- *Ajustar o incorporar nuevos controles conforme a los riesgos identificados.*

Se incorporaron 2 riesgos y 4 controles adicionales, reforzando la cobertura y efectividad de la matriz de riesgos de seguridad de la Información para el siguiente proceso, así:

- ❖ *Proceso Gestión Documental (GD).*

- *Además, es fundamental realizar un seguimiento periódico para verificar el cumplimiento de las medidas adoptadas y garantizar la mejora continua en los procesos.*

Se efectuó seguimiento al cargue de evidencias de controles de seguridad de la información, asegurando la validación de su implementación y el cumplimiento de los lineamientos establecidos para la mejora continua, las evidencias están disponibles para consulta en los repositorios ubicados en la carpeta Share Point.

En todo caso, la validación y actualización del formato F-FI-1385 "Matriz de Riesgos de Seguridad de la Información" se llevará a cabo durante el tercer cuatrimestre, tal como se indicó en el "Informe de Riesgos de Seguridad de la Información Primer Cuatrimestre" consignado en el memorando 3-2025-19176, página 27.

Por lo anterior, de manera respetuosa se solicita que la oportunidad de mejora No. 4 se mantenga vigente durante el cuatrimestre en curso, y no sea incluida para la formulación de un nuevo plan de mejoramiento (Observación 1), considerando que se tiene previsto avanzar en su desarrollo dentro del periodo actual, en concordancia con las acciones que se vienen implementando para fortalecer las recomendaciones emitidas por la Oficina de Control Interno".

Respuesta de la Oficina de Control Interno:

En atención a la respuesta emitida por el proceso auditado, esta Oficina ha realizado el correspondiente análisis técnico y concluye que, si bien se evidencian avances en la revisión de riesgos y la incorporación de nuevos controles, las acciones descritas no atienden de manera específica ni suficiente la observación detectada. En particular, persiste la falta de inclusión de las tipologías de controles automáticos y manuales en la matriz de riesgos de seguridad de la información F-FI-1385 situación que había sido advertida por esta oficina en anteriores seguimientos.

La observación se fundamenta en el incumplimiento de los lineamientos establecidos en los numeral 3.2.2.2 Tipología de controles y los procesos y 3.2.2.3 Análisis y evaluación de los controles– Atributos de la Guía para la administración de los riesgos V6 del DAFP y los numerales 11.7 y 11.7.2 de la Guía de administración de riesgos G-FI-04 V.4 de la Secretaría de Seguridad y Convivencia - SDSCJ, los cuales exigen la clasificación explícita de los controles según su tipología. La ausencia de un campo específico en el formato F-FI-1385 para registrar dicha información continúa limitando su documentación, afectando la trazabilidad, evaluación integral y priorización de acciones de mitigación.

En consecuencia, esta Oficina ratifica la Observación N.º 1 y determina su permanencia para efectos de formulación de un plan de mejora interno, hasta tanto se evidencie el cumplimiento integral de lo observado, incluyendo la actualización estructural del formato F-FI-1385 y la incorporación formal de la tipología de los controles.

Se reconoce el compromiso manifestado por el proceso auditado y se reitera la disposición de esta Oficina para brindar el acompañamiento técnico que se requiera, con el fin de contribuir al fortalecimiento del Sistema de Gestión de Riesgos Institucional.

4.1.7 ETAPA 7: TRATAMIENTO DEL RIESGO RESIDUAL.

Todos los riesgos de seguridad de la información identificados en la Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ, fueron objeto de tratamiento residual, sin excepción, independientemente de la Zona de Riesgo asignada. En la matriz F-FI-1385 de riesgos de seguridad de la información, específicamente en la hoja denominada “TRATAMIENTO DE RIESGO RESIDUAL”, se evidencia que los 35 riesgos registrados fueron categorizados bajo la opción “REDUCIR EL RIESGO”. Esta clasificación uniforme sugiere una estrategia homogénea de tratamiento. Adicionalmente, se observa que, tras la aplicación de los controles definidos, todos los riesgos disminuyen y se ubican en la Zona **BAJO**.

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	1
Atención y Relación con el Ciudadano.	0	0	2
Control Disciplinario.	0	0	2
Direccionamiento Estratégico.	0	0	2

, PROCESO	RIESGO RESIDUAL		
	ALTO	MODERADO	BAJO
Evaluación al Sistema de Control Interno.	0	0	2
Gestión Contractual.	0	0	1
Gestión de Comunicaciones Estratégicas.	0	0	1
Gestión de Emergencias.	0	0	5
Gestión de Seguridad y Convivencia.	0	0	5
Gestión de Tecnologías de la Información.	0	0	2
Gestión Estratégica del Talento Humano.	0	0	2
Gestión Documental	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	1
Gestión y Análisis de la Información.	0	0	1
TOTAL	**0**	**0**	**35**

Tabla N. 7. 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.

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 con el listado de usuarios SIDIJUS II Cuatrimestre 2025, enviado a la Directora de Acceso a la Justicia a través del correo electrónico.	SI

RIESGO #	PROCESO	CONTROL #	CONTROL	SOPORTE	SEGUIMIENTO OCI	CUMPLE
2	Acceso y Fortalecimiento a la Justicia.	1	El profesional y/o los profesionales de la dirección de acceso designados para esta actividad cuatrimestralmente 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 no presentó evidencia de ejecución de la actividad de control correspondiente al segundo cuatrimestre de 2025. Si bien se aportaron informes de verificación y validación de permisos mediante correo electrónico, con fecha del 1 de septiembre de 2025, dicha documentación corresponde al tercer cuatrimestre. **Recomendación:** se requiere soporte específico para cada periodo evaluado, a fin de garantizar la trazabilidad y cumplimiento del ciclo de control.	NO
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 electrónicos y reportes de los meses de mayo, junio, julio y agosto.	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 la DTSI, se debe enviar un correo electrónico y/o comunicado oficial por la Dirección de Bienes solicitando el reporte y/o los motivos de la no entrega de esta información.	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, por otra parte, se observa el correo electrónico solicitando el reporte mensual. **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.	NO

RIESGO #	PROCESO	CONTROL #	CONTROL	SOPORTE	SEGUIMIENTO OCI	CUMPLE
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	Se valida la ejecución de la actividad con los correos electrónicos mensuales (mayo, junio, julio y agosto)	SI
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 con 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	Se valida la ejecución de la actividad con 3 actas del mes de agosto Visita de seguimiento taller y capacitación MOTO MUNDIAL, HYUNDAUTOS S.A.S y INCOLMOTOS YAMAHA S.A y dos listados de asistencia	SI
4	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	La evidencia aportada no permite verificar la actividad de control, ya que el proceso aportó dos memorandos, con el radicado 3-2025-26590 del 4/07/2025 se informa que, se hace necesario contar con un nuevo integrante en el equipo de combustible que contribuya a soportar los requerimientos que desde la administración de dicho sistema se realizan constantemente y ampliar así, la consolidación que desde el área se requiere. Y en el memorando 3-2025-27022 Fecha: 07/07/2025 se indica la suficiencia del personal. No obstante, el proceso no aporta el documento proyección del personal requerido como lo establece el soporte de la evidencia de la actividad de control. **Recomendación**: Formalizar la **proyección del personal requerido** mediante un documento estructurado que permita verificar la actividad de control conforme a los lineamientos establecidos.	NO

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 mayo, junio, julio y agosto 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 29 de agosto, 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 el correo electrónico del 27 de agosto de 2025 asunto: Autorización ingreso a las bases de la OCDI.	SI

RIESGO #	PROCESO	CONTROL #	CONTROL	SOPORTE	SEGUIMIENTO OCI	CUMPLE
8	Control Disciplinario.	1	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. Del periodo mayo a agosto.	SI
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 segundo trimestre de 2025. Asimismo, se presentó el esquema de publicación y los correos electrónicos enviados, con base en dicho esquema.	SI
10	. Direccionamiento Estratégico.	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.	Comunicación oficial y/o correo electrónico	El proceso aportó evidencia de la ejecución de la actividad del control con el correo electrónico asunto: Custodia Actas del Consejo de Seguridad Fecha: jueves, 4 de septiembre de 2025 Sin embargo, dado que la periodicidad establecida para dicha actividad es semestral, no se aportó soporte correspondiente al primer semestre del año 2025, lo que limita la verificación integral del cumplimiento del ciclo completo de control. **Recomendación**: Garantizar el registro semestral de evidencias de control, asegurando soporte específico por cada periodo evaluado.	NO

RIESGO #	PROCESO	CONTROL #	CONTROL	SOPORTE	SEGUIMIENTO OCI	CUMPLE
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 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 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
11	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 evidencio la ejecución de la actividad de control con el memorando con radicado N. 3-2025-187 Fecha: 08/01/2025 en esta misma, se envía la programación para la anualidad para correspondiente cargue.	SI
12	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
13	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 de la anualidad 2025 correspondiente a la información de Archivo Contratos de Jurídica.	SI

RIESGO #	PROCESO	CONTROL #	CONTROL	SOPORTE	SEGUIMIENTO OCI	CUMPLE
14	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 Soporte cambio contraseñas RRSS – SCJ. Fecha Lun 30/06/2025.	SI
15	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 mayo y junio de 2025. También se aportaron dos informes de apoyo y dos de supervisión de mayo y junio, así como los informes de interventoría de mayo y junio; sin embargo, se encuentran pendientes los correspondientes a los meses de julio y agosto de 2025. **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 documentar las gestiones realizadas en caso de ausencia de reportes por parte del operador tecnológico, conforme al procedimiento establecido.	NO
15	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

RIESGO #	PROCESO	CONTROL #	CONTROL	SOPORTE	SEGUIMIENTO OCI	CUMPLE
15	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
16	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 mayo, junio, julio y agosto de 2025	SI
17	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 el reporte documental del periodo junio a julio de 2025 correspondiente a la información mensual del contratista, no obstante, no se aportó la evidencia del mes de agosto. **Recomendación:** se requiere soporte específico para cada periodo evaluado, a fin de garantizar la trazabilidad y cumplimiento del ciclo de control.	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 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 valida la ejecución de la actividad con el correo electrónico con la base de datos incidentes SOARS de mayo a agosto de 2025.	SI

RIESGO #	PROCESO	CONTROL #	CONTROL	SOPORTE	SEGUIMIENTO OCI	CUMPLE
19	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	Se valida la ejecución de la actividad con el correo electrónico Bitácora de transferencia de mando SOARS del 1 de septiembre de 2025 que adjunta cargue correspondiente al segundo cuatrimestre (mayo – agosto).	SI
20	Gestión de Seguridad y Convivencia.	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**	Aunque el proceso aportó el correo electrónico del 29/08/2025 verificación de usuarios activos y roles en Progressus correspondiente al II Cuatrimestre 2025. Se observó que no se aportó la evidencia del reporte de usuarios y roles como se registra en la columna de soportes de la matriz de riesgos de seguridad F-FI-1385. **Recomendación:** Complementar la evidencia de la actividad de control mediante la inclusión del reporte formal de usuarios y roles en Progressus.	NO
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 valida la ejecución de la actividad de control con el correo electrónico del 29/08/2025 actualización de la Guía Progressus.	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 valida la ejecución de la actividad con el acta del 29 de agosto de 2025, en donde se realizó Control y Seguimiento al cargue de documentación Sitio Share Point 220 Dir Seguridad, correspondiente al segundo cuatrimestre 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 valida la ejecución de la actividad con los correos disponibilidad actas de los consejos locales de seguridad de los meses de mayo, junio, julio y agosto de 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 valida la ejecución de la actividad con la matriz verificación y actualización formulario MCyASEE.	SI
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	Se valida la ejecución de la actividad con la tabla verificación registros de actividades territoriales en Survey123.	SI

RIESGO #	PROCESO	CONTROL #	CONTROL	SOPORTE	SEGUIMIENTO OCI	CUMPLE
25	Gestión de Tecnologías de la Información.	1	El responsable de sistema de información verifica de forma cuatrimestral el seguimiento al plan de trabajo de migración 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 contará 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 valida la ejecución de la actividad con el reporte de seguimiento del mes de agosto de 2025.	SI
25	Gestión de Tecnologías de la Información.	2	El responsable de sistema de información realiza seguimiento semestral a la ejecución del plan de actualización documental de la arquitectura de los sistemas de información, en caso de no contar con el seguimiento semestral 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 valida la ejecución de la actividad con los manuales técnicos de los siguientes sistemas (APELACIONES, SIGA, LICO, ARGOS, ORFEO, SCD Videollamada, SIRCAV, PROGRESSUS, DELIVERY, LIMAY, SITIO WEEB, SIRPA, SISIPEC, SAE, SAI, SISCO, TERCEROS II, OPGET, PREDIS, SIDIJUS, SIMBA Y CASA LIBERTAD)	SI
26	Gestión de Tecnologías de la Información.	1	El responsable de infraestructura y el responsable de seguridad de la Información define de forma cuatrimestral el mecanismo seguro y estandarizado para la gestión de credenciales de administración en la infraestructura tecnológica, así como el seguimiento de los mecanismos establecidos, en caso de no contar con el seguimiento a los mecanismos establecidos, se contará con correo electrónico 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 correo electrónico.	Mecanismo de gestión segura de contraseñas o comunicado oficial	Se valida la ejecución de la Actividad con los mecanismos seguros y estandarizados para la gestión de credenciales de administración en la infraestructura tecnológica como: mecanismo autenticación multifactor (MFA), Correo institucional, Mecanismo Controlador de dominio SCJ, Directorio activo, Mecanismo de autenticación interno VPN y Mecanismo portal cautivo.	SI
26	Gestión de Tecnologías de la Información.	2	El responsable de infraestructura tecnológica realiza seguimiento mensual al rendimiento de herramientas de seguridad informática que protegen la información de la SDSCJ, en caso de no hacer seguimiento al rendimiento se contará con correo electrónico 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 correo electrónico.	Reporte de rendimiento de la infraestructura de seguridad o comunicado oficial	Se valida la ejecución de la actividad con el Reporte de rendimiento de la infraestructura de seguridad de los meses de mayo, junio, julio y agosto de 2025.	SI

RIESGO #	PROCESO	CONTROL #	CONTROL	SOPORTE	SEGUIMIENTO OCI	CUMPLE
27	Gestión Documental	1	El profesional restaurador de la Dirección de Recursos Físicos y Gestión Documental, de forma trimestral, valida el informe de Monitoreo de condiciones ambientales de humedad relativa y temperatura y los reportes de limpieza que se realizan en las cajas de la bodega elaborado por el contratista responsable del arrendamiento del inmueble de la bodega de archivo central, en cumplimiento de las cláusulas contractuales y de la normatividad archivística en vigencia; en caso de que el contratista no realice y/o haga entrega oportuna del informe, no se realiza el pago de la factura del periodo, como evidencia queda el correo electrónico de validación del informe presentado.	Informe de Monitoreo Condiciones Ambientales	Se valida la ejecución de la actividad con los Informes de Monitoreo Condiciones Ambientales de los meses de mayo, junio, julio y agosto de 2025	SI
27	Gestión Documental	2	El profesional restaurador de la Dirección de Recursos Físicos y Gestión Documental valida, de forma trimestral, el informe de Mantenimiento locativo que realiza el contratista responsable del arrendamiento del inmueble de la bodega de archivo central, en cumplimiento de las cláusulas contractuales y de la normatividad archivística en vigencia; en caso de que el contratista no realice y/o haga entrega oportuna del informe, no se realiza el pago de la factura del periodo, como evidencia queda el correo electrónico de validación del informe presentado.	Informe de Mantenimiento Locativo	Se valida la ejecución de la actividad con los informes de mantenimiento locativo de los meses de mayo, junio, julio y agosto de 2025.	SI
27	Gestión Documental	3	El profesional del archivo central de la Dirección de Recursos Físicos y Gestión Documental, cada vez que se requiera realiza la digitalización de documentos del Archivo Central que es consultada, de lo cual se conforma un repositorio de copias de respaldo digital de los documentos físicos consultados. En caso de que no se pueda realizar la digitalización de documentos por fallas relacionadas con el componente tecnológico, se realizará la solicitud formal a la Dirección de Tecnologías y sistemas de la información para atender los requerimientos, Como evidencia se entrega la matriz base de datos control de préstamo documental correspondiente a la digitalización de archivos, el cargue de evidencias se realizara de forma cuatrimestral	Matriz de Base de datos control préstamo de documentos	Se valida la ejecución de la actividad con la Matriz de Base de datos control préstamo de documentos.	SI

RIESGO #	PROCESO	CONTROL #	CONTROL	SOPORTE	SEGUIMIENTO OCI	CUMPLE
28	Gestión Documental	1	El administrador Funcional de la Dirección de Recursos Físicos y Gestión Documental de la plataforma SIGA, realiza de forma mensual la verificación de la asignación de usuarios, perfiles, controles de reserva parametrizados en los módulos de comunicaciones y gestión de expedientes para controlar el acceso a la información, a través del módulo de administración de la herramienta y las tablas de control de acceso de la Entidad. En caso de no realizar la verificación mensual por ausencia de personal se informa mediante correo electrónico y/o comunicado oficial al Director de DRFGD para asignación de personal. Como evidencia se presentará el reporte de permisos asignados en los módulos de correspondencia y gestión de expedientes.	Reporte de permisos asignados en los módulos de correspondencia y gestión de expedientes.	Se valida la ejecución de la actividad con los reportes de permisos de los módulos correspondencia y expedientes.	SI
29	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 valida la ejecución de la actividad con los siguientes 4 correos: 1. Correo creación usuario SIAP del 15/07/2025. 2. Correo creación usuario SIAP 2 del 15/07/2025. 3. Correo actualización permisos del 25/08/2025 4. Correo permisos usuarios del 2/07/2025	SI
30	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 valida la ejecución de la actividad con los formatos base consulta y prestamos de las historias laborales de los meses de mayo, junio, julio y agosto de 2025	SI

RIESGO #	PROCESO	CONTROL #	CONTROL	SOPORTE	SEGUIMIENTO OCI	CUMPLE
31	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	La periodicidad definida para la actividad es "cada vez que se requiera"; por tanto, si bien las evidencias aportadas corresponden a septiembre y se encuentran por fuera del periodo de seguimiento, ello no constituye un incumplimiento, dado que la frecuencia establecida no exige una ejecución periódica fija: 1. Correo Solicitud Usuario PREDIS – SICAPITAL del 8/09/2025 2. Correo Solicitud Usuario Publicación SITIO WEB del 8/09/2025	SI
32	Gestión Integral a las Personas Privadas de la Libertad - PPL.	1	El/la funcionario y/o contratista del área jurídica encargado del archivo, a demanda del personal del Centro Especial de Reclusión, atenderá y validará las solicitudes de préstamos de hojas de vida de PPL y demás documentos relacionados. Para lo cual es necesario diligenciar el formato "Consulta y Préstamo Documental Archivo Cárcel Distrital y Centro Especial De Reclusión-CER (F-GIP-1394)". Para casos excepcionales en razón y función del servicio, con autorización expresa de la Dirección del CER los documentos podrán ser entregados sin el diligenciamiento del mencionado formato y dicha autorización deberá quedar por correo electrónico. Las evidencias se reportarán de forma cuatrimestral.	**memorando y/o correo electrónico**	Aunque el proceso aportó el formato "Consulta y Préstamo Documental Archivo Cárcel Distrital y Centro Especial De Reclusión-CER (F-GIP-1394), no se tiene evidencia del correo electrónico o memorando que se registra en la columna soportes de la matriz de riesgos de seguridad F-FI-1385. **Recomendación:** Complementar la evidencia de la actividad de control mediante la inclusión del memorando o correo electrónico, o modificar el soporte registrado en el matriz de riesgo que guarde coherencia con la actividad prevista a ejecutar.	NO
33	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 valida la ejecución de la actividad con el reporte de Excel que incluye el inventario documental de la DJC	SI

RIESGO #	PROCESO	CONTROL #	CONTROL	SOPORTE	SEGUIMIENTO OCI	CUMPLE
34	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	El proceso aportó los Informes de mantenimiento de los meses de abril, mayo, junio y julio, pero no se evidenció el del mes de agosto. Por tanto, se observa una ejecución parcial. **Recomendación:** Efectuar el cargue completo de las evidencias que sustentan el desarrollo de la actividad de control.	NO
34	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	El proceso aportó los Informes de Interventoría de los meses de abril, mayo, junio y julio, pero no se evidenció el del mes de agosto. Por tanto, se observa una ejecución parcial. **Recomendación:** Efectuar el cargue completo de las evidencias que sustentan el desarrollo de la actividad de control.	NO
35	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	Se valida la ejecución de la actividad de control con la medición del indicador MIPG.	SI

Tabla N. 8. 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 ejecución de los 47 controles establecidos, se evidenció que 37 (78,72 %) se cumplieron, mientras que 10 (21,27 %) presentaron debilidades. En relación con los controles que registraron observaciones, resulta necesario atender las recomendaciones consignadas en la tabla anterior, con el propósito de fortalecer su efectividad y mitigar los riesgos asociados.

Respecto de la **OBSERVACIÓN N. 3 – DEBILIDADES FRENTE AL CUMPLIMIENTO DEL NUMERAL ETAPA 8. MONITOREO, REVISIÓN Y REPORTE DE LA GUÍA DE ADMINISTRACIÓN DE LOS RIESGOS G-FI-04 V3**, señalada en el Informe de Seguimiento a los Riesgos de Seguridad de la Información del I Cuatrimestre de 2025 (Radicado N. 3-2025-24957 del 27 de junio de 2025), se evidenció mejora en el reporte de evidencias entre el primer y segundo cuatrimestre: de 12 observaciones sobre 43 controles en el primer periodo, a 10 observaciones sobre 47 controles en el segundo. Sin embargo, persisten observaciones relacionadas con la ausencia de soportes documentales, lo cual limita la verificación integral del cumplimiento de la etapa de monitoreo, revisión y reporte. No obstante, se constató que dicha inconsistencia está siendo abordada mediante la acción definida en el **Plan de Mejora N. 558,** actualmente en términos de ejecución, cuya fecha de finalización está prevista para el 31 de diciembre de 2025, mencionado lo anterior, dicha situación será objeto de seguimiento en el siguiente cuatrimestre.

5. CONCLUSIONES

- En relación con la consistencia metodológica en la identificación y valoración de riesgos, se evidenció que los riesgos están correctamente vinculados a activos específicos, con causas, amenazas y vulnerabilidades claramente diferenciadas, lo cual refleja una aplicación adecuada de la metodología definida en la Guía G-FI-04 V4 y la Política PO-FI-02 V3.

- Se observan avances en identificación y valoración de activos, toda vez que, se ha fortalecido la clasificación de activos según criterios de criticidad (confidencialidad, integridad y disponibilidad), aunque se mantiene pendiente la publicación de la versión actualizada de la matriz F-GD-1081.

- Se subsanó la oportunidad de mejora relacionada con la ausencia de riesgos y controles en el proceso de Gestión Documental, evidenciando capacidad de respuesta ante incidentes previos.

- Se evidencia un leve avance en la ejecución de controles y en la reducción de observaciones frente al primer cuatrimestre de 12 observaciones / 43 controles (28%) a 10 observaciones / 47controles (21%), lo que refleja una mejora en la gestión documental y operativa de los riesgos de seguridad de la información.

- Persistencia de brechas en soportes documentales. A pesar de los avances, continúan observándose inconsistencias en el cargue de evidencias, especialmente en la etapa de monitoreo, revisión y reporte, lo cual limita la trazabilidad y verificación de la actividad de control.

- Los planes de mejora específicos (N.º 556, 557, 558), con fecha de cierre prevista para el 31 de diciembre de 2025, serán objeto de verificación para el tercer cuatrimestre 2025.

6. RECOMENDACIONES

- Emitir y publicar la versión actualizada de la matriz de activos de información (F-GD-1081), incorporando los ajustes realizados, para garantizar visibilidad, trazabilidad y alineación con principios de acceso a la información.

- Realizar seguimiento técnico y administrativo a los planes de mejora N.º 556, 557 y 558, asegurando su ejecución dentro del plazo previsto y documentando los resultados alcanzados.

- Optimizar la articulación entre líneas de defensa, mejorando la coordinación entre la primera y segunda línea de defensa para garantizar la consistencia entre los controles implementados y los soportes cargados, facilitando la labor de auditoría de la tercera línea.

- Efectuar la inclusión de todos los procesos institucionales en los registros de activos y riesgos, evitando omisiones que puedan comprometer la cobertura del sistema de gestión de riesgos.

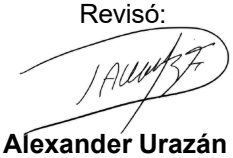
- Se recomienda iniciar la transición metodológica hacia la implementación de la Guía para la Gestión Integral del Riesgo – Versión 7, adoptando de manera progresiva lo que señala la Guía, respecto a los riesgos de seguridad de la información, la cual incorpora nuevos enfoques en materia de apetito, tolerancia y capacidad de riesgo, así como una gestión más integral de los riesgos tecnológicos y de ciberseguridad.

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