ALCALDÍA MAYOR DE BOGOTÁ
SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA
AL RESPONDER CITAR EL NR.
Nro. Rad: 3-2026-3367
Fecha: 15/01/2026 10:46:00 AM
Destino: 130-OCI

MEMORANDO

Para: IVAN ARTURO MARQUEZ RINCON
OFICINA DE CONTROL INTERNO

De: DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION

Asunto: INFORME TERCER CUATRIMESTRE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN - 2025

Respetada Doctor: Marquez.

En cumplimiento de la Política de Administración de Riesgos de la Secretaría Distrital de Seguridad, Convivencia y Justicia, y en atención a las directrices establecidas por el Departamento Administrativo de la Función Pública, de manera respetuosa se remite el informe cuatrimestral adjunto sobre Riesgos de Seguridad de la Información.

Este informe tiene como propósito su revisión y posterior socialización en el ámbito de su responsabilidad.

Agradecemos de antemano sus consideraciones y comentarios al respecto.

Quedamos a su disposición para cualquier aclaración o consulta adicional.

Cordialmente,

IVAN HERSAYN PINILLA HERRERA
DIRECTOR DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION

c.c.e.: EDWIN CASTILLO ORTIZ-DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION
RAFAEL HUMBERTO LOPEZ SAAVEDRA-DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION
JORGE ELIECER VELASQUEZ PERILLA-DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION
FRANCISCO ALFORD BOJACA-COBRO PERSUASIVO
OSCAR ALBERTO PORRAS MURCIA-EQUIPO ATENCION AL CIUDADANO
RAFAEL MAURICIO SOPO SOLANO-DIRECCION DE RECURSOS FISICOS Y GESTION DOCUMENTAL
MARIA ALEJANDRA LOPEZ FAGUA-DIRECCION DE RECURSOS FISICOS Y GESTION DOCUMENTAL
PATRICIA GOMEZ VELASQUEZ-DIRECCION DE RECURSOS FISICOS Y GESTION DOCUMENTAL

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

JULIAN PONTON SILVA-OFICINA ASESORA DE PLANEACION
DAMIAN CAMILO VARGAS VARGAS-OFICINA ASESORA DE PLANEACION
PAOLA ANDREA CHACON TELLEZ-OFICINA ASESORA DE COMUNICACIONES
YESSICA PAOLA NOGUERA BECERRA-OFICINA ASESORA DE COMUNICACIONES
SOONYI ALEJANDRA MUNOZ TORRES-OFICINA DE CONTROL INTERNO
HECTOR ARMANDO OSPINA OSPINA-OFICINA DE CONTROL DISCIPLINARIO INTERNO
JENNIFER CATHERINE VELASQUEZ-OFICINA DE CONTROL DISCIPLINARIO INTERNO
JUAN FELIPE CAMPOS CONTRERAS-OFICINA DE ANÁLISIS DE INFORMACION Y ESTUDIOS ESTRATEGICOS
DIANA MARCELA FLECHAS RUIZ-OFICINA DE ANÁLISIS DE INFORMACION Y ESTUDIOS ESTRATEGICOS
ADA LUZ SANDOVAL HERAZO-OFICINA CENTRO COMANDO, CONTROL, COMUNICACIONES Y COMPUTO C-4
ANA CATHERINE MARINO RINCON-OFICINA CENTRO COMANDO, CONTROL, COMUNICACIONES Y COMPUTO C-4
CLARA JOHANNA VELEZ RODRIGUEZ-OFICINA CENTRO COMANDO, CONTROL, COMUNICACIONES Y COMPUTO C-4
ALBERTO SANCHEZ GALEANO-SUBSECRETARIA DE SEGURIDAD Y CONVIVENCIA
SANDRA MILENA PEREZ RAMIREZ-SUBSECRETARIA DE SEGURIDAD Y CONVIVENCIA
ALEJANDRO REYES LOZANO-DIRECCION DE PREVENCION Y CULTURA CIUDADANA
LINA MARIA TORO TAMAYO.-SUBSECRETARIA DE ACCESO A LA JUSTICIA
KATHERINE PAOLA HERRERA MORENO-DIRECCION DE ACCESO A LA JUSTICIA
IVAN ARTURO TORRES ARANGUREN-DIRECCION DE RESPONSABILIDAD PENAL ADOLESCENTE
RICHARD OSVALDO GONZALEZ VERA-DIRECCION DE BIENES PARA LA SEGURIDAD, CONVIVENCIA Y ACCESO A LA JUSTICIA
DEIDER MAURICIO MENGUAL PATERNINA.-SUBSECRETARIA DE GESTION INSTITUCIONAL
VILMA PATRICIA FERREIRA LUGO-DIRECCION DE GESTION HUMANA
PIEDAD CONSTANZA PARDO RODRIGUEZ-DIRECCION DE GESTION HUMANA
DEISY NATALIA VALENCIA GONZALEZ-DIRECCION FINANCIERA
MAURICIO MOSQUERA GOMEZ-DIRECCION DEL CENTRO ESPECIAL DE RECLUSION

Anexos: -1

Elaboró: DIEGO MAURICIO USME GONZALEZ
Revisó: JUAN PABLO RIVERA SALAMANCA-DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION -
Aprobó: IVAN HERSAYN PINILLA HERRERA

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

ALCALDÍA MAYOR DE BOGOTÁ D.C.

BOGOTÁ

Dirección de Tecnologias y Sistemas de la Información

INFORME DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN TERCER CUATRIMESTRE - 2025

Contenido

INTRODUCCIÓN

De conformidad con lo establecido en la Política de Administración de Riesgos de la Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ (PO-FI-02 - Ver. 3), particularmente en el ítem 11 sobre Publicación, Seguimiento y Evaluación de los Riesgos, la Dirección de Tecnologías y Sistemas de la Información, en su calidad de Segunda Línea de Defensa, tiene la responsabilidad de efectuar el seguimiento cuatrimestral a la Matriz de Riesgos de Seguridad de la Información y remitir el informe correspondiente a la Oficina de Control Interno dentro de los diez (10) días hábiles siguientes al cierre de cada cuatrimestre. En cumplimiento de lo anterior, el presente documento consolida y expone las actividades de seguimiento realizadas durante el tercer cuatrimestre de la vigencia 2025, con el fin de garantizar la trazabilidad, control y evaluación de los riesgos asociados a la seguridad de la información en la Entidad.

El seguimiento a la matriz de riesgos de seguridad de la información se fundamenta en el proceso previo de levantamiento de activos aprobado y publicado en la vigencia 2025, en el cual se validaron 281 activos de información. Estos fueron evaluados por el personal responsable de cada proceso, con base en los principios de Confidencialidad, Integridad y Disponibilidad. Como resultado, se clasificaron 71 activos con criticidad Alta, 150 con criticidad Media y 60 con criticidad Baja.

Cabe resaltar que, en coordinación con la Dirección de Recursos Físicos y Gestión Documental y la Dirección de Tecnologías y Sistemas de la Información, se llevaron a cabo mesas de trabajo orientadas al plan de actualización de activos de información. Como resultado, al cierre del tercer cuatrimestre se logró la validación y actualización de los activos de información correspondientes de los 21 procesos, los cuales, fueron publicados en el sitio web institucional y en datos abiertos Bogotá para la vigencia 2025.

A partir de los 71 activos clasificados con criticidad alta, se identificaron y estructuraron 36 riesgos asociados a la seguridad de la información, para los cuales se definieron un total de 50 controles aplicables a toda la Entidad.

Este ejercicio se desarrolló siguiendo los lineamientos definidos en la Política de Administración de Riesgos institucional, para los siguientes procesos:

TIPO DE PROCESOS	PROCESOS
Estratégicos	Atención y Relación con el Ciudadano. (AR)
	Direccionamiento estratégico (DE)
	Gestión de Comunicaciones Estratégicas. (GCE)
	Gestión de Tecnología de la Información (GT).
	Gestión y Análisis de la Información (GI).
	Gestión Estratégica del Talento Humano (GH).
Misionales	Acceso y Fortalecimiento a la Justicia (AJ)
	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas. (AB)

	Gestión de Emergencia (GE)
	Gestión Integral a las Personas Privadas de la Libertad - PPL. (GIP)
	Gestión de Seguridad y Convivencia (GS)
	Gestión Tecnológica de Seguridad y Emergencias. (GST)
Apoyo	Gestión Contractual (GC)
	Gestión Financiera. (GF)
	Gestión Jurídica (GJ)
	Gestión Documental (GD)
De Evaluación	Evaluación al Sistema de Control Interno (SM)
	Control Disciplinario (CID)

Tabla.1 Procesos SDSCJ.

En líneas generales, cada uno de los procesos y áreas mencionadas se ha detectado al menos un riesgo, y todos ellos están en conformidad con los lineamientos establecidos en la Política de Administración de Riesgos PO-FI-02 Ver. 3 adoptada por la SDSCJ.

1. Conocimiento y Divulgación.

En el mes de diciembre de 2025, la Dirección de Tecnologías y Sistemas de la Información (DTSI) llevó a cabo el diseño y la divulgación de una pieza gráfica titulada "¡Seguridad de la Información Responsabilidad de todos!", la cual fue difundida de manera masiva a toda la Entidad como parte de sus actividades de socialización. La evidencia correspondiente está disponible en el siguiente enlace:

https://scjgovcol.sharepoint.com/:f:/r/sites/DireccionTIC/Documentos%20compartidos/GobiernoTI/MIPG/Riesgos/Seguridad%20Informaci%C3%B3n/2025/Informes/Tercer%20Cuatrimestre/Pieza%20Grafica?csf=1&web=1&e=yvxvag

Gráfica.1 Elaboración Uso y Apropiación DTSI.

Adicionalmente, la Dirección de Tecnologías y Sistemas de la Información (DTSI) emitió el memorando electrónico digital 3-2025-49759 del 09 de diciembre de 2025, En este informe se proporciona información sobre el cargue de evidencias asociadas a los controles implementados para la mitigación de los riesgos de seguridad de la información, correspondientes a los meses de septiembre, octubre, noviembre y diciembre (tercer cuatrimestre de la vigencia 2025), dirigidas a los procesos y áreas previamente definidos en la Matriz de Riesgos de la Entidad. El enlace para acceder a dicha información es el siguiente:

https://scjgovcol.sharepoint.com/:f:/r/sites/DireccionTIC/Documentos%20compartidos/GobiernoTI/MIPG/Riesgos/Seguridad%20Informaci%C3%B3n/2025/Informes/Tercer%20Cuatrimestre/Memorando?csf=1&web=1&e=b10aT0

Asimismo, se efectuó la difusión institucional de la información mediante comunicación oficial enviada por correo electrónico a todas las áreas responsables de la gestión de riesgos de seguridad de la información. Esta comunicación tuvo como propósito brindar instrucciones para el cargue de evidencias correspondientes al tercer cuatrimestre y, de manera complementaria, dar a conocer la validación de las observaciones formuladas por la Oficina de Control Interno en relación con el informe de riesgos de seguridad de la información del segundo cuatrimestre de 2025, garantizando así la retroalimentación y fortalecimiento de las actividades de seguimiento. Las evidencias están disponibles en el siguiente enlace:

https://scjgovcol.sharepoint.com/:f:/r/sites/DireccionTIC/Documentos%20compartidos/GobiernoTI/MIPG/Riesgos/Seguridad%20Informaci%C3%B3n/2025/Informes/Tercer%20Cuatrimestre/Comunicaciones%20Electronicas?csf=1&web=1&e=ktDwku

2. Identificación de los Activos de Seguridad de la Información.

Durante la vigencia 2025, la Dirección de Recursos Físicos y Gestión Documental, en articulación con la Dirección de Tecnologías y Sistemas de la Información, adelantó mesas de trabajo con la totalidad de los procesos y áreas de la Entidad, orientadas a la actualización de los activos de información, en concordancia con la actualización de las Tablas de Retención Documental (TRD).

Dichas actividades se desarrollaron mediante sesiones presenciales y virtuales con cada una de las áreas, en las cuales se socializaron de manera detallada las directrices, lineamientos y responsabilidades asociadas al diligenciamiento del formato F-GD-1081 “Registro de Activos de Información e Índice de Información Clasificada y Reservada”.

Como resultado de estas jornadas, se logró la consolidación de la información requerida, apoyada en la realización de ejercicios prácticos orientados al levantamiento, validación y actualización de los activos de información por proceso. A partir de este ejercicio integral, se consolidó la siguiente información:

Proceso	Criticidad Alta	Criticidad Media	Criticidad Baja	Total, Activo
Atención y Relación con el Ciudadano	0	5	8	13
Direccionamiento Estratégico	8	7	0	15
Fortalecimiento Institucional	0	1	0	1
Gestión del Conocimiento y la Innovación Pública	0	1	2	3
Gestión y Análisis de la Información	1	3	0	4
Gestión de Comunicaciones Estratégicas	1	6	0	7
Gestión de Tecnologías de la Información	4	4	1	9
Gestión Estratégica del Talento Humano	8	6	2	16
Gestión de Emergencias	7	1	0	8
Gestión Tecnológica de Seguridad y Emergencias	2	0	0	2
Gestión de Seguridad y Convivencia	10	13	0	23
Acceso y Fortalecimiento a la Justicia	7	8	0	15
Gestión Integral a las Personas Privadas de la Libertad - PPL	2	39	40	81
Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas	5	4	1	10
Evaluación al Sistema de Control Interno	2	9	1	12
Control Disciplinario	5	0	0	5
Gestión Contractual	2	0	1	3
Gestión Jurídica	5	1	0	6
Gestión de Recursos Físicos al Servicio de la Entidad	0	15	0	15
Gestión Documental	2	4	4	10
Gestión Financiera	0	23	0	23
Total	**71**	**150**	**60**	**281**

Tabla. 2 Activos Información SDSCJ.

En este sentido, se indica que la actualización del Registro de Activos de Información y el Índice de Información Clasificada y Reservada se encuentra publicada en la página web de la Entidad a través del siguiente enlace:

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

Las evidencias de la publicación de los activos de información en el portal de datos abiertos Bogotá se encuentra en el siguiente enlace:

https://datosabiertos.bogota.gov.co/dataset/https-scj-gov-co-transparencia-datos-abiertos-registros-activos-informacion

3. Identificación del riesgo.

Para el tercer cuatrimestre del 2025, se dio gestión y actualización a la "Matriz de Riesgos de Seguridad de la información", la cual está disponible en la página WEB de la SDSCJ, en la siguiente ruta:

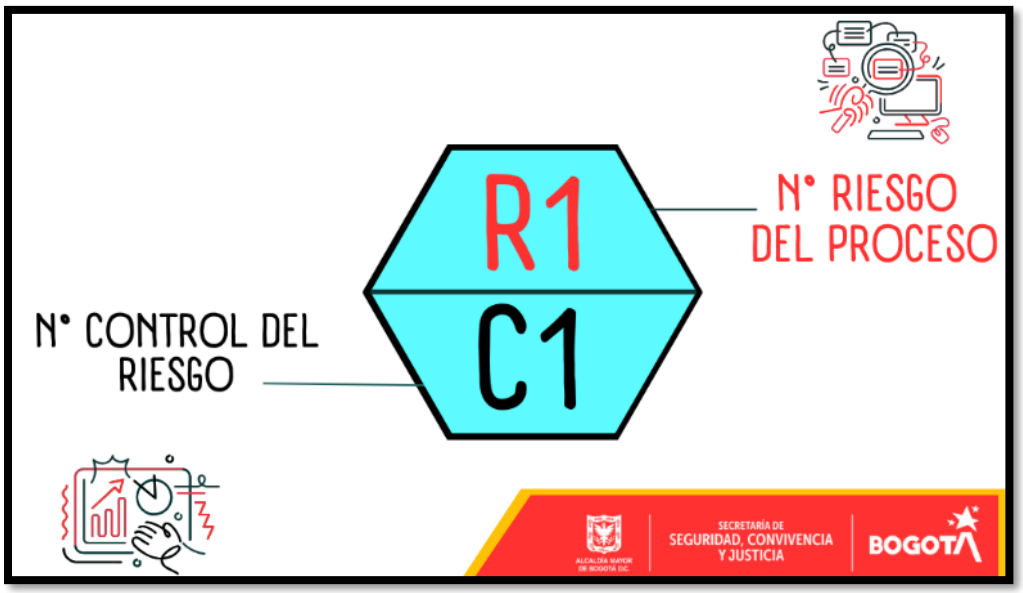
- **WEB**: https://scj.gov.co/es Transparencia y Acceso a la información pública - Planeación, políticas lineamientos y manuales -Plan de acción - Matriz de riesgos Seguridad de la Información – 2025.
  https://scj.gov.co/transparencia/planeacion-presupuesto-ingresos/plan-accion?field_action_plan_classification_target_id=367&field_class_anti_plan_citizen_se_target_id=All&field_public_expen_plan_class_target_id=All&field_class_strate_secto_ins_pla_target_id=All&field_general_date_value=&title=

Los siguientes son los lineamientos generales para la gestión de los Riesgos de seguridad de la información:

- Se dispone de una (1) Matriz General de Riesgos de Seguridad de la Información, en la cual se consolida y agrupa la totalidad de los riesgos asociados a los procesos de la Entidad, incluyendo la información correspondiente a la hoja de resumen, el inventario de activos de información, la identificación del riesgo inherente, la definición del tratamiento del riesgo, la valoración del riesgo con la aplicación de controles, así como la determinación y tratamiento del riesgo residual.

- Todos los riesgos y sus respectivos controles se encuentran alineados con la metodología definida en la Política de Administración de Riesgos de la Entidad.

- La nomenclatura asignada a cada riesgo corresponde a la siguiente referencia:



Grafica 2. Nomenclatura Riesgos.

Los Riesgos de seguridad de la información se agrupan por Procesos de la siguiente forma:

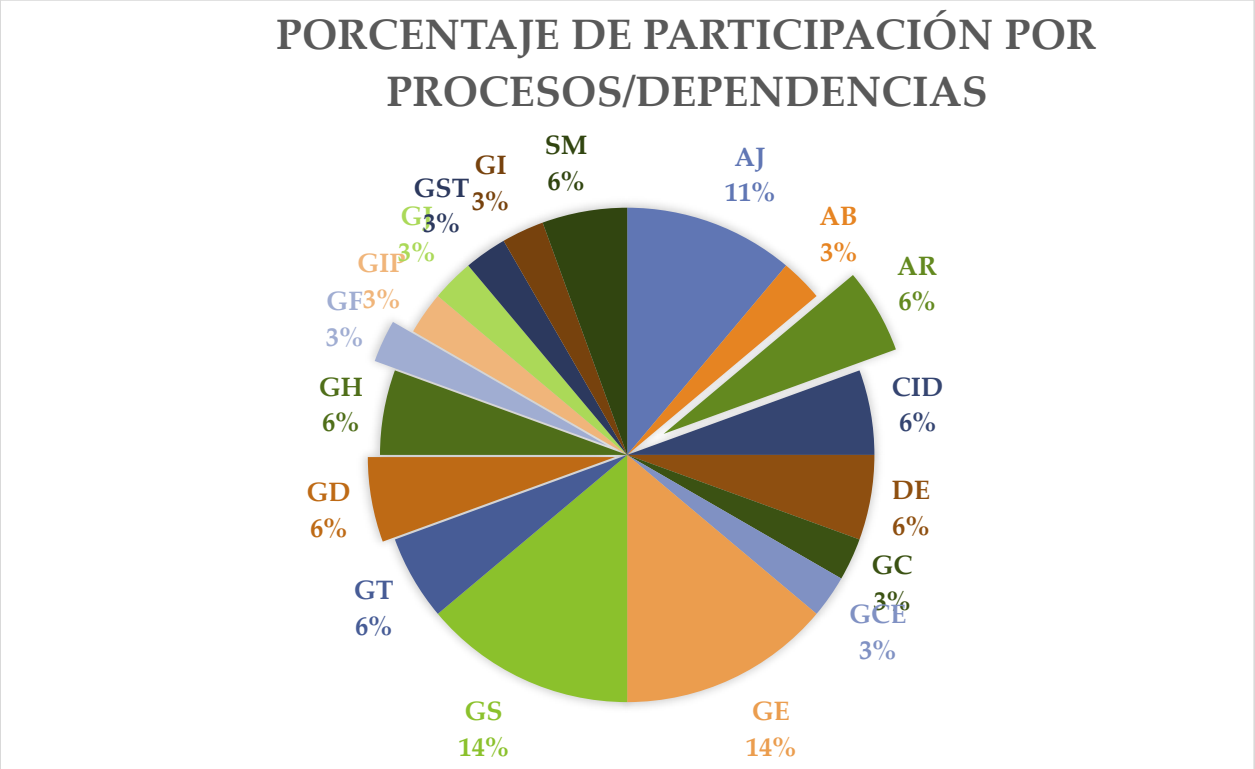
PROCESO	SIGLA	RIESGOS
Acceso y Fortalecimiento a la Justicia	AJ	4
Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	AB	1
Atención y Relación con el Ciudadano.	AR	2
Control Disciplinario.	CID	2
Direccionamiento Estratégico.	DE	2
Evaluación al Sistema de Control Interno.	SM	2
Gestión Contractual	GC	1
Gestión de Comunicaciones Estratégicas.	GCE	1
Gestión de Emergencias	GE	5
Gestión de Seguridad y Convivencia	GS	5
Gestión de Tecnología de Información	GT	2
Gestión Documental.	GD	2
Gestión Estratégica del Talento Humano.	GH	2
Gestión Financiera.	GF	1
Gestión Integral a las Personas Privadas de la Libertad - PPL.	GIP	1
Gestión Jurídica	GJ	1
Gestión Tecnológica de Seguridad y Emergencias.	GST	1
Gestión y Análisis de Información	GI	1
	Total Riesgos	**36**

Tabla 3. Procesos Riesgos de Seguridad de Información.

En referencia a los riesgos de seguridad de la información definidos para el tercer cuatrimestre de la vigencia 2025, se evidencia, al cierre del periodo, un incremento de un (1) riesgo de seguridad de la información, con dos (2) controles asociados, correspondiente al proceso de Acceso y Fortalecimiento a la Justicia.

Dicho incremento obedece al fortalecimiento del ejercicio de identificación y análisis de riesgos, derivado de la actualización de la Matriz de Riesgos de Seguridad de la Información y de la revisión detallada de los activos de información críticos del proceso, lo cual permitió identificar de manera más precisa nuevas situaciones de riesgo que anteriormente no se encontraban formalmente documentadas.

Porcentaje de Participación por Procesos/dependencias



Grafica 3. Porcentaje de Participación por Procesos/dependencias

4. Valoración del riesgo.

Continuando con la gestión del riesgo se determina la valoración del riesgo, que se obtiene con la estimación de la probabilidad de ocurrencia e impacto a razón de los siguientes rangos:

Tabla Criterio de Probabilidad

Nivel de Probabilidad	Frecuencia de la actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximo 1 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 2 a 1.000 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 1.001 a 5.000 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 5.001 veces al año y máximo 10.000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 10.001 veces por año	100%

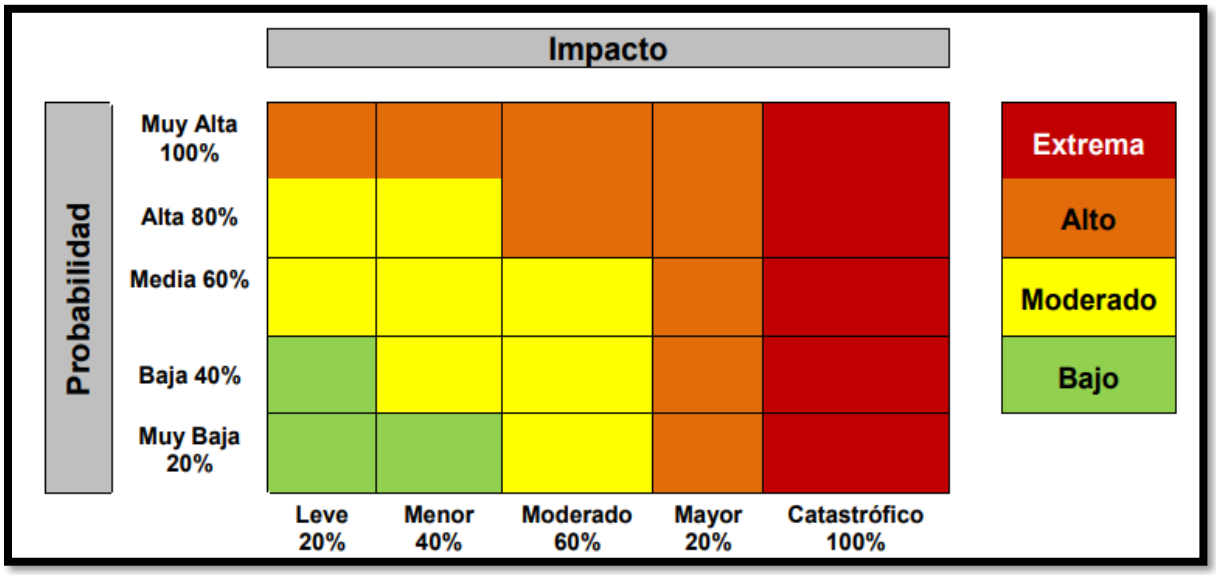
Grafica 4. Fuente: Política de Administración de Riesgos SDSCJ.

Tabla Criterio de impacto

Niveles de Impacto	Afectación Económica	Afectación Reputacional	Impacto
Leve	Afectación menor a 49.999 SMLMV	El riesgo afecta la imagen de algún área de la organización.	20%
Menor	Entre 50.000 y 99.999 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.	40%
Moderado	Entre 100.000 y 199.999 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.	60%
Mayor	Entre 200.000 y 299.999 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.	80%
Catastrófico	Mayor a 300.000 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país	100%

Grafica 5. Fuente: Política de Administración de Riesgos SDSCJ.

Lo anterior, permite la ubicación en el mapa de calor constituido de la siguiente forma:



Grafica 6. Fuente: Política de Administración de Riesgos SDSCJ.

Todas las valoraciones fueron realizadas por los Líderes de Proceso o Líderes Operativos, en conjunto con sus respectivos equipos de trabajo, y contaron con el acompañamiento y la orientación de la Dirección de Tecnologías y Sistemas de la Información. Las valoraciones de Probabilidad e Impacto obtenidas permitieron determinar la Zona de Riesgo Inherente, cuyos resultados se presentan en el siguiente cuadro:

PROCESO	EXTREMO	ALTO	MODERADO	BAJA	Total
Acceso y Fortalecimiento a la Justicia (AJ)			3	1	4
Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas. (AB)			1		1
Atención y Relación con el Ciudadano (AR)			2		2
Control Disciplinario (CID)			2		2
Direccionamiento Estratégico. (DE)		1	1		2
Evaluación al Sistema de Control Interno (SM)			2		2
Gestión Contractual (GC)			1		1
Gestión de Comunicaciones Estratégicas. (GCE)			1		1
Gestión de Emergencias (GE)			5		5
Gestión de Seguridad y Convivencia (GS)			5		5
Gestión de Tecnología de Información (GT)		2			2
Gestión Documental (GD)			1	1	2
Gestión Estratégica del Talento Humano (GH)			2		2
Gestión Financiera. (GF)			1		1
Gestión Integral a las Personas Privadas de la Libertad - PPL. (GIP)			1		1
Gestión Jurídica (GJ)			1		1
Gestión Tecnológica de Seguridad y Emergencias. (GST)			1		1
Gestión y Análisis de Información (GI)		1			1
Total	**0**	**4**	**30**	**2**	**36**

Tabla 4. Valoración Riesgos SDSCJ

Teniendo en cuenta la necesidad de garantizar la continuidad operativa y la adecuada ejecución de los procedimientos definidos en los procesos de la Entidad, no se adoptó la opción de tratamiento “Evitar” para los riesgos identificados. En su lugar, los procesos optaron por la estrategia de “Reducir el riesgo”, la cual consiste en la implementación y fortalecimiento de controles orientados a disminuir la probabilidad de ocurrencia y/o el impacto de los riesgos, en concordancia con lo establecido en la Política de Administración de Riesgos de la Entidad.

A continuación, se presenta la cantidad de riesgos y controles identificados por cada proceso.

Es importante precisar que el número de controles definidos no guarda una relación directa con la materialización de los riesgos. Dichos controles han sido establecidos por cada proceso de acuerdo con su análisis, criterio técnico y recursos disponibles, con el objetivo de prevenir y mitigar, en la medida de lo posible, la ocurrencia y el impacto de los riesgos identificados.

Proceso	N° Riesgos	N° Controles
Acceso y Fortalecimiento a la Justicia (AJ)	**4**	**5**
Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas. (AB)	**1**	**4**
Atención y Relación con el Ciudadano (AR)	**2**	**2**
Control Disciplinario (CID)	**2**	**2**
Direccionamiento Estratégico. (DE)	**2**	**2**
Evaluación al Sistema de Control Interno (SM)	**2**	**3**
Gestión Contractual (GC)	**1**	**1**
Gestión de Comunicaciones Estratégicas. (GCE)	**1**	**1**
Gestión de Emergencias (GE)	**5**	**7**
Gestión de Seguridad y Convivencia (GS)	**5**	**6**
Gestión de Tecnología de Información (GT)	**2**	**4**
Gestión Documental (GD)	**2**	**4**
Gestión Estratégica del Talento Humano (GH)	**2**	**2**
Gestión Financiera. (GF)	**1**	**1**
Gestión Integral a las Personas Privadas de la Libertad - PPL. (GIP)	**1**	**1**
Gestión Jurídica (GJ)	**1**	**1**
Gestión Tecnológica de Seguridad y Emergencias. (GST)	**1**	**2**
Gestión y Análisis de Información (GI)	**1**	**2**
Total	**36**	**50**

Tabla 5. Riesgos y Controles

En referencia a los controles de seguridad de la información establecidos para el tercer cuatrimestre de la vigencia 2025, al cierre del periodo se evidenció un incremento de tres (3) controles, de los cuales dos (2) corresponden al proceso de Acceso y Fortalecimiento a la Justicia y uno (1) al proceso de Gestión y Análisis de la Información.

Este incremento se deriva del fortalecimiento en la identificación y formalización de controles, como resultado de la actualización de la Matriz de Riesgos de Seguridad de la Información y del análisis de los riesgos asociados a los activos de información críticos de dichos procesos, con el propósito de robustecer los mecanismos de prevención y mitigación frente a posibles incidentes de seguridad de la información.

5. Creación de Controles.

Tomando como referencia las mesas de trabajo con las áreas y/o procesos descritos en el Ítem anterior sobre las recomendaciones establecidas por la Oficina de Control Interno, se presentan los ajustes en la Matriz de Riesgos de Seguridad de la Información, así:

# Riesgo	Proceso/Dependencia	Riesgo	Control
R1-C1	Acceso y Fortalecimiento a la Justicia	Pérdida de la Integridad	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.
R2-C1	Acceso y Fortalecimiento a la Justicia	Pérdida de la Confidencialidad	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.
R3-C1	Acceso y Fortalecimiento a la Justicia	Pérdida de la Integridad	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.
R4-C1	Acceso y Fortalecimiento a la Justicia	Pérdida de la Integridad Pérdida de la Confidencialidad	El profesional asignado por la Subsecretaria de Acceso a la Justicia verifica de forma mensual los permisos de acceso de los usuarios a la base de datos del programa Casa libertad de acuerdo con los roles y responsabilidades. En caso de identificar usuarios sin la debida autorización se debe solicitar la aprobación formal de acceso o proceder con la revocación de los permisos correspondientes, como evidencia del control, se remite al jefe del área correo electrónico con el reporte de los permisos a la base de datos del programa Casa Libertad.
R4-C2	Acceso y Fortalecimiento a la Justicia	Pérdida de la Integridad Pérdida de la Confidencialidad	El profesional asignado por la Subsecretaria de Acceso a la Justicia valida de forma mensual la ejecución de la copia de seguridad de la base de datos del programa Casa Libertad en el repositorio designado. En caso de no realiza las actividades de respaldo, se debe informar al jefe del área los motivos del incumplimiento y las acciones implementadas para la ejecución oportuna de la copia de seguridad. Como evidencia del control se remite al jefe del área correo electrónico que documente la ejecución de la copia de seguridad de la base de datos del programa Casa Libertad.
R5-C1	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	Pérdida de la Integridad	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.
R5-C2	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	Pérdida de la Integridad	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.

R5-C3	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	Pérdida de la Integridad	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.
R5-C4	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	Pérdida de la Integridad	El articulador de cada área funcional de la Dirección de Bienes realiza, de manera semestral, la verificación de la disponibilidad del personal asignado para la operación del sistema de información para la Administración de Bienes SIMBA. Como resultado de esta revisión, informa al Director de Bienes, mediante correo electrónico y/o memorando, las necesidades de personal requeridas para asegurar la correcta ejecución y continuidad de las funciones asociadas al sistema. La evidencia del control corresponde a la comunicación formal bien sea mediante correo electrónico y/o memorando enviado al Director de Bienes. En caso de que la operación cuente con el personal completo y no se requieran ajustes, esta condición también será documentada mediante correo electrónico dirigido al Director de Bienes.
R6-C1	Atención y Relación con el Ciudadano.	Pérdida de la Integridad Perdida de Confidencialidad	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.
R7-C1	Atención y Relación con el Ciudadano.	Pérdida de la Integridad Perdida de Confidencialidad	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.
R8-C1	Control Disciplinario.	Pérdida de la Integridad	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.
R9-C1	Control Disciplinario.	Pérdida de la Confidencialidad	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.
R10-C1	Direccionamiento Estratégico.	Pérdida de la Disponibilidad	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.
R11-C1	Direccionamiento Estratégico.	Pérdida de la Confidencialidad	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.
R12-C1	Evaluación al Sistema de Control Interno.	Pérdida de la Integridad	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.
R12-C2	Evaluación al Sistema de Control Interno.	Pérdida de la Integridad	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.
R13-C1	Evaluación al Sistema de Control Interno.	Pérdida de la Integridad	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.
R14-C1	Gestión Contractual.	Pérdida de la Disponibilidad Perdida de la Integridad	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.
R15-C1	Gestión de Comunicaciones Estratégicas.	Pérdida de la Confidencialidad y Perdida de la Integridad	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.
R16-C1	Gestión de Emergencias	Pérdida de la Confidencialidad	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.
R16-C2	Gestión de Emergencias	Pérdida de la Confidencialidad	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.
R16-C3	Gestión de Emergencias	Pérdida de la Confidencialidad	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.

R17-C1	Gestión de Emergencias	Pérdida de la Disponibilidad	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.
R18-C1	Gestión de Emergencias	Pérdida de Confidencialidad, Integridad y/o disponibilidad de la información	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.
R19-C1	Gestión de Emergencias	Pérdida de la Disponibilidad	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.
R20-C1	Gestión de Emergencias	Pérdida de la Disponibilidad	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.
R21-C1	Gestión de Seguridad y Convivencia	Perdida de la Integridad y Disponibilidad	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.
R21-C2	Gestión de Seguridad y Convivencia	Perdida de la Integridad y Disponibilidad	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.
R22-C1	Gestión de Seguridad y Convivencia	Pérdida de la Confidencialidad	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.
R23-C1	Gestión de Seguridad y Convivencia	Pérdida de la Disponibilidad	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.

R24-C1	Gestión de Seguridad y Convivencia	Pérdida de la Confidencialidad	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.
R25-C1	Gestión de Seguridad y Convivencia	Pérdida de la Integridad	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.
R26-C1	Gestión de Tecnología de Información	Pérdida de Confidencialidad, integridad y/o disponibilidad de la información	"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."
R26-C2	Gestión de Tecnología de Información	Pérdida de Confidencialidad, integridad y/o disponibilidad de la información	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
R27-C1	Gestión de Tecnología de Información	Pérdida de Confidencialidad, integridad y/o disponibilidad de la información	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.
R27-C2	Gestión de Tecnología de Información	Pérdida de Confidencialidad, integridad y/o disponibilidad de la información	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.
R28-C1	Gestión Documental.	Pérdida de la Disponibilidad	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.
R28-C2	Gestión Documental.	Pérdida de la Disponibilidad	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.
R28-C3	Gestión Documental.	Pérdida de la Disponibilidad	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
R29-C1	Gestión Documental.	Perdida de la Confidencialidad Perdida de la Integridad	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.
R30-C1	Gestión Estratégica del Talento Humano.	Pérdida de la Integridad	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.
R31-C1	Gestión Estratégica del Talento Humano.	Pérdida de la Confidencialidad	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
R32-C1	Gestión Financiera.	Pérdida de la Integridad	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.
R33-C1	Gestión Integral a las Personas Privadas de la Libertad - PPL.	Pérdida de la Disponibilidad Perdida de Confidencialidad	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.
R34-C1	Gestión Jurídica.	Pérdida de la Disponibilidad Perdida de la Confidencialidad Perdida de la Integridad	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.
R35-C1	Gestión Tecnológica de Seguridad y Emergencias.	Pérdida de Confidencialidad, Integridad y/o	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

		disponibilidad de la información	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.
R35-C2	Gestión Tecnológica de Seguridad y Emergencias.	Pérdida de Confidencialidad, Integridad y/o disponibilidad de la información	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.
R36-C1	Gestión y Análisis de la Información.	Pérdida de la Integridad	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.
R36-C2	Gestión y Análisis de la Información.	Pérdida de la Integridad	"El Profesional Universitario, Especializado y/o Contratista de la Oficina de Análisis de Información y Estudios Estratégicos responsable de la bodega de datos, verifica de forma Cuatrimestral, con el personal administrador de la base de datos, la asignación de permisos de usuario, roles y trazabilidad en la bodega de datos con el fin de validar que solo las personas autorizadas se encuentre con usuario activo de acuerdo a las responsabilidades asignadas, como evidencia del control, el responsable envía correo electrónico al jefe del a OAIEE, con el listado actualizado de usuarios activos especificando el tipo de acceso, permisos y trazabilidad de las acciones realizadas por cada usuario; En caso de identificar usuarios sin autorización, se deberán retirar los permisos de acceso de manera inmediata y reportar las acciones realizadas al Jefe de la Oficina. "

Tabla 6. Estructuración de Controles.

En el seguimiento a los riesgos y controles de seguridad de la información del tercer cuatrimestre de la vigencia 2025, se evidenció la incorporación de dos (2) controles para el proceso de Acceso y Fortalecimiento a la Justicia (R4-C1 y R4-C2), así como un (1) control adicional para el proceso de Gestión y Análisis de la Información (R36-C2), como resultado del fortalecimiento del análisis de riesgos y de la actualización de la Matriz de Riesgos de Seguridad de la Información.

Los ajustes a la matriz de riesgos de seguridad de la Información serán cargados en el sitio web de la Entidad, de acuerdo con los parámetros establecidos en la Política de Administración de Riesgos en el siguiente enlace:

https://scj.gov.co/transparencia/planeacion-presupuesto-ingresos/plan-accion?field_action_plan_classification_target_id=367&field_class_anti_plan_citizen_se_target_id=All&field_public_expen_plan_class_target_id=All&field_class_strate_secto_ins_pla_target_id=All&field_general_date_value=&title=

6. Tratamiento del Riesgo Residual.

La Dirección de Tecnologías y Sistemas de la Información (DTSI) brindó un acompañamiento permanente a los procesos de la Entidad, con el propósito de apoyar el cumplimiento de los lineamientos asociados a la gestión de los riesgos de seguridad de la información. Dicho acompañamiento se desarrolló mediante orientación técnica, articulación y coordinación interprocesos, y seguimiento continuo a las actividades definidas, lo cual permitió fortalecer la implementación y efectividad de los controles establecidos.

Gracias a este trabajo articulado, se logró la implementación efectiva de las medidas de tratamiento del riesgo, lo cual contribuyó de manera significativa a la mitigación de las amenazas identificadas y al fortalecimiento de la gestión del riesgo de seguridad de la información a nivel institucional.

Los resultados de la gestión realizada se evidencian a través del análisis comparativo entre la Zona de Riesgo Inherente y la Zona de Riesgo Residual, el cual se presenta en el siguiente cuadro y permite visualizar la efectividad de los controles implementados por cada proceso.

PROCESO	INHERENTE				RESIDUAL			
	EXTREMO	ALTO	MODERADO	BAJA	EXTREMO	ALTO	MODERADO	BAJA
Acceso y Fortalecimiento a la Justicia (AJ)			3	1				4
Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas. (AB)			1					1
Atención y Relación con el Ciudadano (AR)			2					2
Control Disciplinario (CID)			2					2
Direccionamiento Estratégico. (DE)		1	1					2
Evaluación al Sistema de Control Interno (SM)			2					2
Gestión Contractual (GC)			1					1
Gestión de Comunicaciones Estratégicas. (GCE)			1					1
Gestión de Emergencias (GE)			5					5
Gestión de Seguridad y Convivencia (GS)			5					5
Gestión de Tecnología de Información (GT)		2						2
Gestión Documental (GD)			1	1				2
Gestión Estratégica del Talento Humano (GH)			2					2
Gestión Financiera. (GF)			1					1
Gestión Integral a las Personas Privadas de la Libertad - PPL. (GIP)			1					1
Gestión Jurídica (GJ)			1					1
Gestión Tecnológica de Seguridad y Emergencias. (GST)			1					1
Gestión y Análisis de Información (GI)		1						1
Total	**0**	**4**	**30**	**2**	**0**	**0**	**0**	**36**

Tabla 7. Zona de Riesgo Inherente y Zona de Riesgo Residual

7. Monitoreo, revisión y reporte.

En atención a las observaciones y oportunidades de mejoras emitidas por la Oficina de Control Interno (OCI) a través del memorando # 3-2025-42443, correspondiente al "Informe de seguimiento a riesgos de seguridad de la información - segundo cuatrimestre de 2025", se llevaron a cabo mesas de trabajo con las áreas involucradas, con el fin de validar y ajustar la evaluación de los controles y las evidencias presentadas:

7.1 Observaciones Oficina Control Interno – Segundo Cuatrimestre.

7.1.1 **OBSERVACIÓN N° 1** Falta de inclusión de tipologías de controles automáticos y manuales en la matriz de riesgos de seguridad de la información 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.

En atención a la oportunidad de mejora relacionada con la ausencia de la diferenciación entre 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 la definición, clasificación y aplicación de los controles, en concordancia con las recomendaciones formuladas por la Oficina de Control Interno.

En este marco, se realizó la validación, ajuste y actualización del formato F-FI-1385 – Matriz de Riesgos de Seguridad de la Información, versión 2, incorporando mejoras en la identificación y tipificación de los controles, con el fin de robustecer la gestión del riesgo. Dicho formato fue revisado y validado por el Grupo de Estrategia de la Dirección de Tecnologías y Sistemas de la Información (DTSI) y, posteriormente, propuesto para su aprobación y publicación en el portal MIPG, garantizando su alineación con la política institucional de administración de riesgos y los lineamientos vigentes en materia de seguridad de la información.

Las evidencias están disponibles para consulta en los repositorios ubicados en la carpeta Share Point:

https://scjgovcol.sharepoint.com/:f:/r/sites/DireccionTIC/Documentos%20compartidos/GobiernoTI/MIPG/Riesgos/Seguridad%20Informaci%C3%B3n/2025/Informes/Tercer%20Cuatrimestre/Matriz%20Riegos?csf=1&web=1&e=l4zfqa

De igual forma, se llevaron a cabo mesas de trabajo con los diferentes procesos institucionales para la socialización de la actualización de la Matriz de Riesgos de Seguridad de la Información, en las cuales se presentaron los ajustes efectuados al formato F-FI-1385 – Matriz de Riesgos de Seguridad de la Información. Dichos ajustes incluyeron la actualización de la misión, visión, objetivos estratégicos y recursos asociados, así como la incorporación de la tipología de los controles (manuales y automáticos), en atención a los requerimientos formulados por la Oficina de Control Interno, con el propósito de fortalecer la gestión y el entendimiento integral de los riesgos de seguridad de la información al interior de la Entidad.

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:

- Acceso y Fortalecimiento a la Justicia.
- Administración De Bienes Muebles E Inmuebles Para El Fortalecimiento De Las Capacidades Operativas (AB).
- Gestión de Emergencias.
- Gestión de Seguridad y Convivencia.
- Gestión Tecnológica de Seguridad y Emergencias (GST).
- Gestión Integral a las Personas Privadas de la Libertad - PPL.

Adicionalmente, se incorporaron 1 riesgos y 3 controles adicionales, reforzando la cobertura y efectividad de la matriz de riesgos de seguridad de la Información, así:

- Acceso y Fortalecimiento a la Justicia.
- Gestión y Análisis de la Información.

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.

Las evidencias están disponibles para consulta en los repositorios ubicados en la carpeta Share Point:

https://scjgovcol.sharepoint.com/:f:/r/sites/DireccionTIC/Documentos%20compartidos/GobiernoTI/MIPG/Riesgos/Seguridad%20Informaci%C3%B3n/2025/Informes/Tercer%20Cuatrimestre/Mesas%20Trabajo?csf=1&web=1&e=vQCZT4

7.1.2 Observación 3: debilidades frente al cumplimiento de la numeral etapa 8. monitoreo, revisión y reporte de la guía de administración de los riesgos g-fi-04 v3

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

7.1.2.1 Proceso Acceso y Fortalecimiento a la Justicia.

- Recomendación riesgo 2 – control 1: Revisión y ajustes de evidencias

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.

Atención a recomendación:

Para esta recomendación, se aclara que, si bien la documentación fue presentada con fecha 01/09/2025, corresponde efectivamente a la información del segundo cuatrimestre de 2025. La entrega fuera de las fechas establecidas se debió a la consolidación de los registros requeridos, pero refleja de manera completa y fiel las actividades y controles ejecutados durante dicho periodo. Para el tercer cuatrimestre, la entrega de evidencias se realizará conforme a las consideraciones y lineamientos establecidos por la Oficina de Control Interno, garantizando la trazabilidad y el cumplimiento del ciclo de control.

Para esta recomendación, se informa por parte del equipo de trabajo del proceso Acceso y Fortalecimiento a la Justicia (AJ), se establece que en el próximo cumplimiento del tercer cuatrimestre de riesgos de seguridad de Información se presentara de acuerdo con las recomendaciones de la OCI.

Gráfica 7. Cargue Evidencias Riesgo 2 – Control 2

7.1.2.2 Proceso Administración De Bienes Muebles E Inmuebles Para El Fortalecimiento De Las Capacidades Operativas (AB).

- Recomendación riesgo 4 – control 1: Revisión y ajustes de evidencias.

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.

Atención a recomendación:

Para la presente recomendación, el grupo estructurador del proceso Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas (AB) informa que, como parte de la desviación identificada, se presentó el memorando 3-2025-71114. Así mismo, se precisa que en el próximo cumplimiento del cargue de evidencias correspondiente al tercer cuatrimestre de la vigencia 2025, se presentarán las evidencias del cargue del control, de conformidad con las recomendaciones emitidas por la OCI.

Gráfica 8. Cargue Evidencias Riesgo 4 – Control 1

- Recomendación Riesgo 4 – Control 4: Revisión y ajustes de evidencias.

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.

De acuerdo con las recomendaciones del informe de seguimiento de riesgos de seguridad de la información correspondiente al segundo cuatrimestre, el grupo estructurador, con el apoyo de la DTSI, y a partir de las revisiones y análisis realizados al control, propone los siguientes ajustes al mismo:

Control Actual:

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.

Ajustes al Control 4:

El articulador de cada área funcional de la Dirección de Bienes realiza, de manera semestral, la verificación de la disponibilidad del personal asignado para la operación del sistema de información para la Administración de Bienes SIMBA. Como resultado de esta revisión, informa al Director de Bienes, mediante correo electrónico y/o memorando, las necesidades de personal requeridas para asegurar la correcta ejecución y continuidad de las funciones asociadas al sistema. La evidencia del control corresponde a la comunicación formal bien sea mediante correo electrónico y/o memorando enviado al Director de Bienes. En caso de que la operación cuente con el personal completo y no se requieran ajustes, esta condición también será documentada mediante correo electrónico dirigido al Director de Bienes.

Así mismo, se precisa que en el próximo cumplimiento del cargue de evidencias correspondiente al tercer cuatrimestre de la vigencia 2025, se presentarán las evidencias del cargue del control, de conformidad con las recomendaciones emitidas por la OCI.

5	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	4	Reducir el riesgo	Gestión deficiente de las contraseñas.	Interrupción de los sistemas / procesos	El articulador de cada área funcional de la Dirección de Bienes realiza, de manera semestral, la verificación de la disponibilidad del personal asignado para la operación del sistema de información para la Administración de Bienes SIMBA. Como resultado de esta revisión, informa al Director de Bienes, mediante correo electrónico y/o memorando, las necesidades de personal requeridas para asegurar la correcta ejecución y continuidad de las funciones asociadas al sistema. La evidencia del control corresponde a la comunicación formal bien sea mediante correo electrónico y/o memorando enviado al Director de Bienes. En caso de que la operación cuente con el personal completo y no se requieran ajustes, esta condición también será documentada mediante correo electrónico dirigido al Director de Bienes.	Preventivo	Manual

Gráfica 9. Cargue Evidencias Riesgo 4 – Control 4

7.1.2.3 Proceso Direccionamiento estratégico

- Recomendación riesgo 10 - control 1: Revisión y ajustes de evidencias.

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.

Atención a recomendación:

En atención a la recomendación formulada para el riesgo R10, control C1, correspondiente al seguimiento del primer cuatrimestre de los riesgos de seguridad de la información, se informa que la evidencia relacionada con la custodia de las actas del Consejo de Seguridad fue cargada oportunamente durante el primer semestre en los repositorios establecidos. No obstante, dichas evidencias fueron inicialmente asociadas al riesgo R19, control C1, conforme a la versión vigente de la Matriz de Riesgos de Seguridad de la Información para el primer cuatrimestre.

Posteriormente, y de acuerdo con las consideraciones definidas y las actualizaciones validadas en el formato F-FI-1385 – Matriz de Riesgos de Seguridad de la Información, durante el segundo cuatrimestre este riesgo fue reclasificado como R10, control C1. En consecuencia, la información y evidencia correspondiente fueron cargadas y asociadas al control actual, garantizando la trazabilidad y consistencia del seguimiento del riesgo.

Así mismo, se precisa que en el próximo cumplimiento del cargue de evidencias correspondiente al tercer cuatrimestre de la vigencia 2025, se presentarán las evidencias del cargue del control, de conformidad con las recomendaciones emitidas por la OCI.

Gráfica 10. Cargue Evidencias Riesgo 10 – Control 1

7.1.2.4 Proceso de Gestión de Emergencias (GE).

- Recomendación riesgo 15 - control 1: Revisión y ajustes de evidencias.

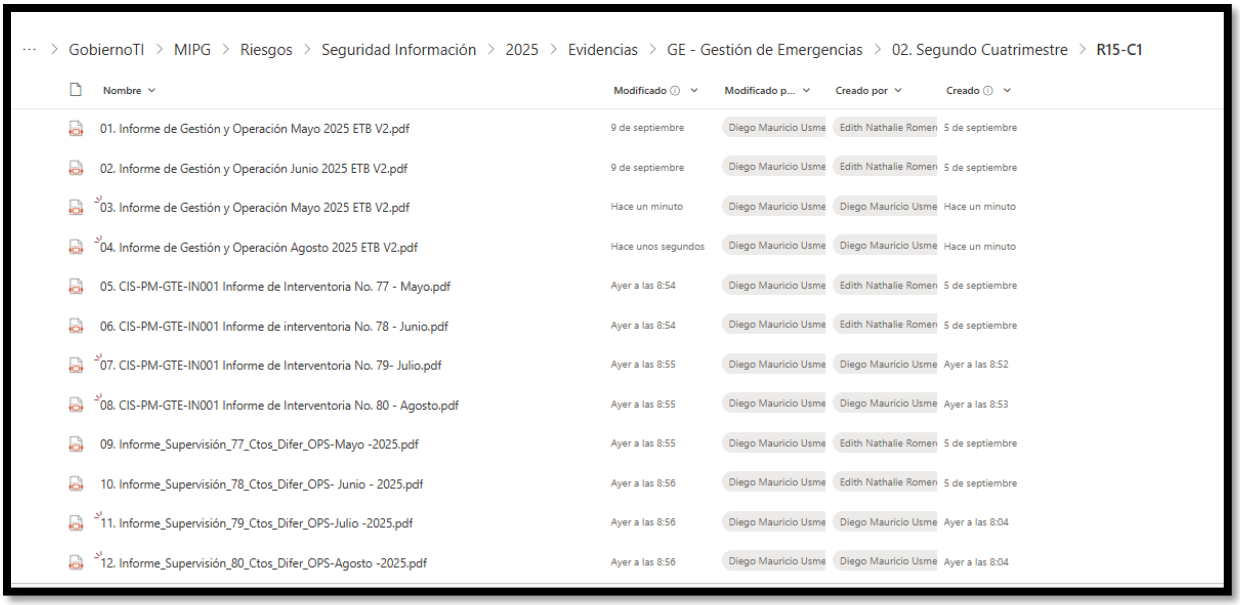
La evidencia aportada no permite verificar la ejecución completa de la actividad de control, ya que el proceso presentó los informes de gestión y operación correspondientes a los meses de mayo y junio de 2025. También se aportaron dos informes de apoyo y dos de supervisión de mayo y junio, así como los 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.

Ajustes a Recomendación:

Para esta recomendación, se informa por parte del equipo de trabajo del proceso de Gestión de Emergencias (GE), se re realiza el cargue de información de acuerdo con las recomendaciones generadas por la OCI.

- Informes de gestión y operación correspondientes a los meses de junio y julio de 2025.
- Informes de apoyo de junio y julio.
- Informe supervisión OPS mes de junio y julio



Grafica 11. Cargue Evidencias R15–C1

Dentro de las evidencias presentadas se establece que en el próximo cumplimiento para el tercer cuatrimestre de riesgos de seguridad de Información se presentara de acuerdo con las recomendaciones de la OCI.

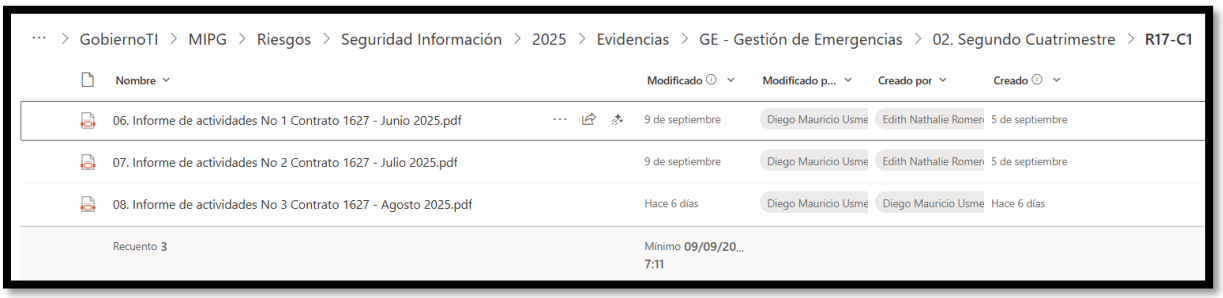
❖ Recomendación riesgo 17 - control 1: Revisión y ajustes de evidencias.

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.

Para esta recomendación, se informa por parte del equipo de trabajo del proceso de Gestión de Emergencias (GE), se re realiza el cargue de información de acuerdo con las recomendaciones generadas por la OCI.

- Informe Mensual de Empresa Contratista mes de agosto.



Grafica 12. Cargue Evidencias R17–C1

7.1.2.5 Proceso Gestión de Seguridad y Convivencia (GS).

❖ Recomendación riesgo 20 – control 1: Revisión y ajustes de evidencias.

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.

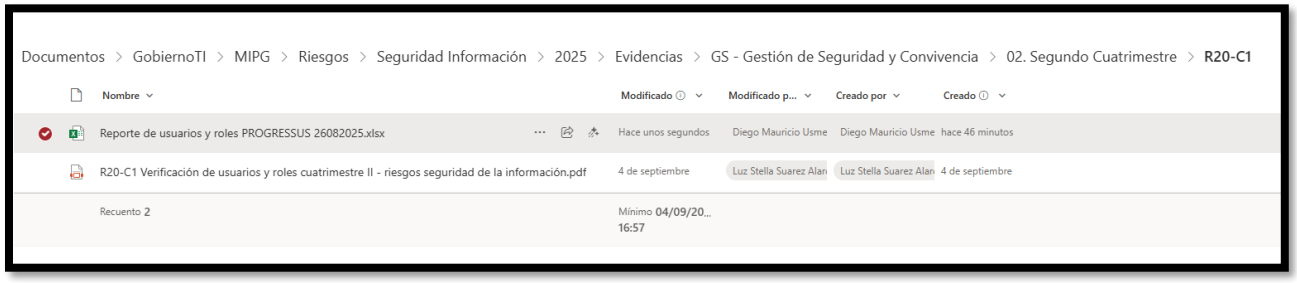
Recomendación: Complementar la evidencia de la actividad de control mediante la inclusión del reporte formal de usuarios y roles en Progressus.

Para esta recomendación, el equipo de trabajo del proceso de Gestión de Seguridad y Convivencia (GS) informa lo siguiente:

Dentro de la respuesta, se debe indicar a la OCI que el listado se encuentra en el correo electrónico del 27/08/2025, como anexo denominado “Solicitud de inactivación de usuarios en PROGRESSUS”, donde se confirma la verificación de los usuarios y se establece la inactivación de los usuarios que ya no requieren permisos en el sistema, por lo que se cumple la intención de la evidencia presentada.

Asimismo, se realizó el cargue de la información conforme a las recomendaciones emitidas por la OCI.

- Reporte de usuarios y roles PROGRESSUS - 26082025



Grafica 13. Cargue Evidencias R20–C1

Para esta recomendación, se realizará el cargue de información de acuerdo con las recomendaciones generadas por la OCI para el corte del tercer cuatrimestre de la vigencia 2025.

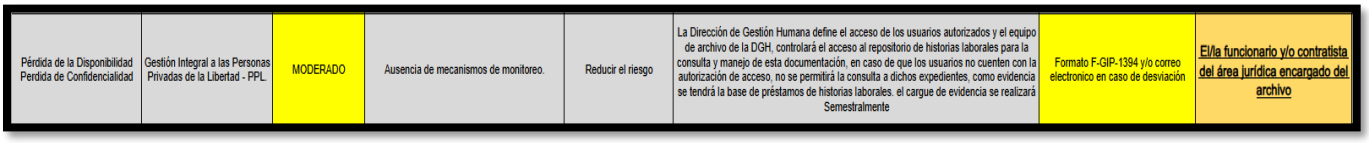
7.1.2.6 Gestión Integral a las Personas Privadas de la Libertad - PPL.

- ❖ Recomendación riesgo 32 - control 1: Revisión y ajustes de evidencias.

Aunque el proceso aportó el formato “Consulta y Préstamo Documental Archivo Cárcel Distrital y Centro Especial De Reclusión-CER (F-GIP1394), 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.

En el ejercicio de la validación de riesgos y controles de seguridad de la información referente al Centro Especial de Reclusión, por parte del equipo estructurador del CER y en apoyo técnico por parte de la DTSI, se establece que el soporte y la evidencia es el formato F-GIP-1394 y el correo electrónico corresponde a los casos de desviación y para el segundo cuatrimestre no se presentan desviaciones a reportar, se realiza los ajustes pertinentes en la matriz de riesgos seguridad de la información referente al tipo de "SOPORTE" de acuerdo a la estructura del control.



Pérdida de la Disponibilidad Perdida de Confidencialidad	Gestión Integral a las Personas Privadas de la Libertad - PPL	MODERADO	Ausencia de mecanismos de monitoreo.	Reducir el riesgo	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	Formato F-GIP-1394 y/o correo electronico en caso de desviación	El/la funcionario y/o contratista del área jurídica encargado del archivo

Grafica 14. Cargue Evidencias R32–C1

Para esta recomendación, se realizará el cargue de información de acuerdo con las recomendaciones generadas por la OCI para el corte del tercer cuatrimestre de la vigencia 2025.

7.1.2.7 Proceso Gestión Tecnológica de Seguridad y Emergencias (GST).

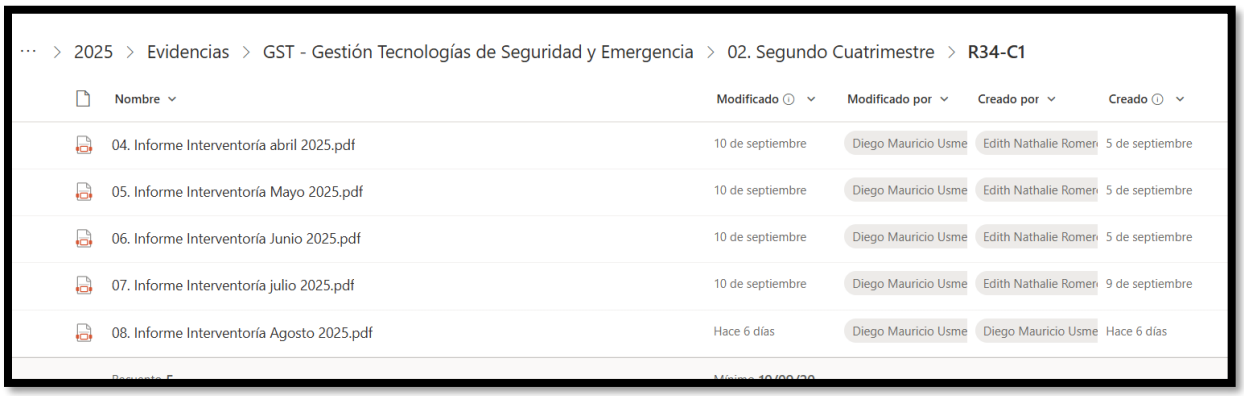
- ❖ Recomendación riesgo 34 - control 1: Revisión y ajustes de evidencias.

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.

Para esta recomendación, se informa por parte del equipo de trabajo del proceso de Gestión de Emergencias (GE), se re realiza el cargue de información de acuerdo con las recomendaciones generadas por la OCI.

- Reporte Mensual Mantenimiento mes Agosto.



Grafica 15. Cargue de Evidencias R34–C1

Dentro de las evidencias presentadas se establece que en el próximo cumplimiento para el tercer cuatrimestre de riesgos de seguridad de Información se presentara de acuerdo con las recomendaciones de la OCI.

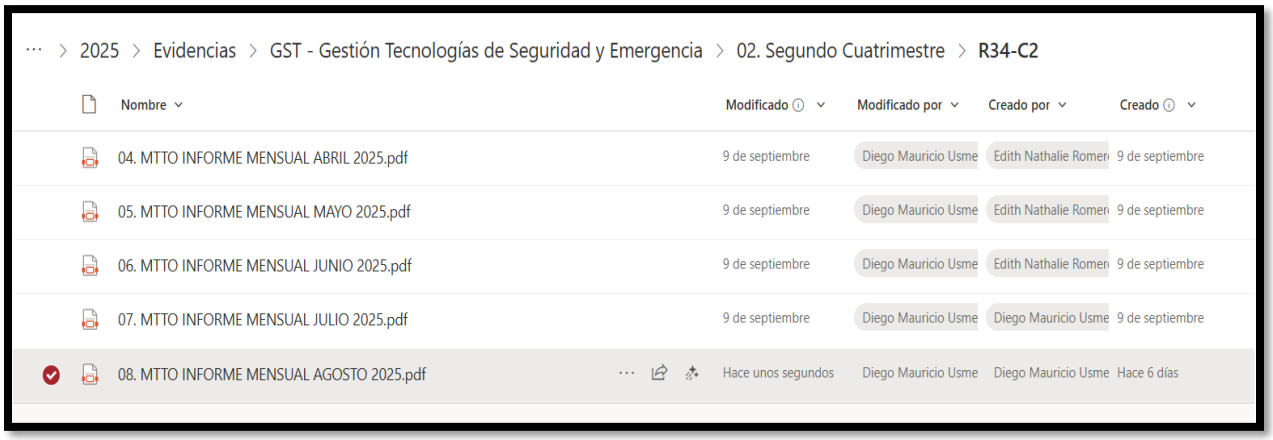
- ❖ Recomendación riesgo 34 - control 2: Revisión y ajustes de evidencias.

Se evidencia la ejecución mensual de los informes de mantenimiento correspondientes a los meses de enero, febrero y marzo de 2025. No obstante, se encuentra pendiente la presentación del informe correspondiente al mes de abril.

Se sugiere realizar el seguimiento respectivo para garantizar la entrega oportuna del informe de abril, a fin de mantener la continuidad y trazabilidad del control establecido.

Para esta recomendación, se informa por parte del equipo de trabajo del proceso de Gestión de Emergencias (GE), se re realiza el cargue de información de acuerdo con las recomendaciones generadas por la OCI.

- Reporte Mensual Mantenimiento mes Agosto.



Grafica 16. Cargue de Evidencias R34–C2

Para esta recomendación, se informa por parte del equipo de trabajo el proceso Gestión Tecnológica de Seguridad y Emergencias (GST), Dentro de las evidencias presentadas se establece que para el tercer cuatrimestre de riesgos de seguridad de Información se entregara de acuerdo con las recomendaciones de la OCI.

Documentación Mesas de Trabajo:

Las mesas de trabajo llevadas a cabo por la Dirección de Tecnologías y Sistemas de la Información, en conjunto con las áreas pertinentes, para la atención de la observación 3: "*debilidades frente al cumplimiento de la numeral etapa 8. monitoreo, revisión y reporte de la guía de administración de los riesgos G-FI-04 v3*" fueron documentadas mediante la elaboración de sus respectivas actas, así:

- Acceso y Fortalecimiento Justicia (AJ).
- Administración De Bienes Muebles E Inmuebles Para El Fortalecimiento De Las Capacidades Operativas (AB).
- Gestión Emergencias (GE)
- Gestión Tecnológica de Seguridad y Emergencias (GST).

Estas actas de las mesas de trabajo de las observaciones del segundo cuatrimestre generadas por la Oficina de Control Interno están disponibles para consulta en los repositorios ubicados en la carpeta Share Point:

https://scjgovcol.sharepoint.com/:f:/r/sites/DireccionTIC/Documentos%20compartidos/GobiernoTI/MIPG/Riesgos/Seguridad%20Informaci%C3%B3n/2025/Informes/Tercer%20Cuatrimestre/Mesas%20Trabajo?csf=1&web=1&e=qi6If9

7.2 Oportunidades de Mejora - Oficina Control Interno – Segundo Cuatrimestre.

7.2.1. Oportunidad de Mejora 1.

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

En relación con la observación Durante la vigencia 2025, la Dirección de Recursos Físicos y Gestión Documental, en coordinación con la Dirección de Tecnologías y Sistemas de la Información, desarrolló mesas de trabajo con todas las áreas y procesos de la Entidad, con el propósito de actualizar los activos de información, en alineación con la revisión y actualización de las Tablas de Retención Documental (TRD).

Estas actividades se llevaron a cabo a través de sesiones presenciales y virtuales, en las cuales se socializaron de forma clara y detallada los lineamientos, orientaciones y responsabilidades relacionadas con el diligenciamiento del formato F-GD-1081 – Registro de Activos de Información e Índice de Información Clasificada y Reservada.

Como resultado de este ejercicio articulado, se logró la recopilación, validación y actualización de la información requerida por cada proceso, apoyándose en ejercicios prácticos que facilitaron la correcta identificación y consolidación de los activos de información institucionales.

En este sentido, se indica que la actualización del Registro de Activos de Información y el Índice de Información Clasificada y Reservada se encuentra publicada en la página web de la Entidad a través del siguiente enlace:

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

Las evidencias de la publicación de los activos de información en el portal de datos abiertos Bogotá se encuentra en el siguiente enlace:

https://datosabiertos.bogota.gov.co/dataset/https-scj-gov-co-transparencia-datos-abiertos-registros-activos-informacion

Documentación Mesas de Trabajo:

Las evidencias de la publicación de los activos de información se pueden consultar en los repositorios ubicados en la carpeta Share Point:

https://scjgovcol.sharepoint.com/:f:/r/sites/DireccionTIC/Documentos%20compartidos/Gobierno TI/MIPG/Riesgos/Seguridad%20Informaci%C3%B3n/2025/Informes/Tercer%20Cuatrimestre/Activos%20Informaci%C3%B3n?csf=1&web=1&e=zzYCnb

8. CARGUE EVIDENCIAS

A través del memorando interno No. 3-2025-49759 del 09 de diciembre de 2025, emitido por la Dirección de Tecnologías y Sistemas de la Información (DTSI), Se solicitó el cargue de la información correspondiente al tercer cuatrimestre de la vigencia 2025, con fundamento en las recomendaciones formuladas en el informe de seguimiento a los controles asociados a los riesgos de seguridad de la información del segundo cuatrimestre de 2025, elaborado por la Oficina de Control Interno. En dicha comunicación se brindaron orientaciones específicas sobre los ajustes requeridos en la entrega y calidad de las evidencias por parte de los procesos y áreas responsables para la vigencia en curso.

De acuerdo con lo establecido en la Política de Administración de Riesgos, se contempla la realización de seguimiento cuatrimestral a la ejecución de los controles de seguridad de la información definidos para todos los procesos. En este sentido, se habilitó para los líderes operativos la carpeta “GobiernoTI/MIPG/Riesgos/SeguridadInformación” en los repositorios de SharePoint de la Entidad, con el fin de facilitar el cargue de las evidencias relacionadas con la implementación de dichos controles.

Mediante el siguiente enlace se puede acceder al repositorio SharePoint disponible para tal fin y verificar la información reportada, así:

https://scjgovcol.sharepoint.com/:f:/r/sites/DireccionTIC/Documentos%20compartidos/GobiernoTI/MIPG/Riesgos/Seguridad%20Informaci%C3%B3n/2025/Evidencias?csf=1&web=1&e=Ibigac

En mencionado repositorio, se puede validar la siguiente información junto con los soportes compartidos para cada riesgo por proceso, así:

Sigla	Proceso	N° Riesgos	Controles	Evidencias publicadas controles
AJ	Acceso y Fortalecimiento a la Justicia	4	R1-C1	2
			R2-C1	2
			R3-C1	8
			R4-C1	1
			R4-C2	1
AB	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas	1	R5-C1	4
			R5-C2	4
			R5-C3	3
			R5-C4	3
AR	Atención y Relación con el Ciudadano	2	R6-C1	14
			R7-C1	3
CID	Control Disciplinario	2	R8-C1	2
			R9-C1	1
DE	Direccionamiento Estratégico.	2	R10-C1	5

			R11-C1	4
SM	Evaluación al Sistema de Control Interno	2	R12-C1	2
			R12-C2	2
			R13-C1	2
GC	Gestión Contractual	1	R14-C1	2
GCE	Gestión de Comunicaciones Estratégicas.	1	R15-C1	4
GE	Gestión de Emergencias	5	R16-C1	12
			R16-C2	17
			R16-C3	1
			R17-C1	19
			R18-C1	12
			R19-C1	2
			R20-C1	2
GS	Gestión de Seguridad y Convivencia	5	R21-C1	2
			R21-C2	2
			R22-C1	1
			R23-C1	4
			R24-C1	1
			R25-C1	1
GT	Gestión de Tecnología de Información	2	R26-C1	1
			R26-C2	30
			R27-C1	6
			R27-C2	12
GD	Gestión Documental	2	R28-C1	4
			R28-C2	4
			R28-C3	1
			R29-C1	2
GH	Gestión Estratégica del Talento Humano	2	R30-C1	7
			R31-C1	3
GF	Gestión Financiera	1	R32-C1	1
GIP	Gestión Integral a las Personas Privadas de la Libertad - PPL	1	R33-C1	1
GJ	Gestión Jurídica	1	R34-C1	1
GST	Gestión Tecnológica de Seguridad y Emergencias	1	R35-C1	4
			R35-C2	4
GI	Gestión y Análisis de Información	1	R36-C1	5
			R36-C2	2
	Total	**36**	**50**	**233**

Tabla 8. Cargue Evidencias.

Lo anterior evidencia que los líderes de proceso cumplieron satisfactoriamente con la entrega de las evidencias correspondientes a la ejecución de los controles, con base en los soportes

suministrados. De esta manera, se confirma la destacada gestión realizada, en términos generales, por los procesos de la Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ en lo relacionado con la Administración y Gestión de los Riesgos de Seguridad de la Información.

9. CONCLUSIONES

En conclusión, al cierre del tercer cuatrimestre de la vigencia 2025, la Dirección de Tecnologías y Sistemas de la Información (DTSI) ratifica su compromiso con la gestión integral de la seguridad de la información, mediante la revisión, actualización y seguimiento permanente de la Matriz de Riesgos de Seguridad de la Información, en concordancia con la Política de Administración de Riesgos de la Entidad.

La implementación de dicha política en materia de seguridad de la información ha sido liderada por la DTSI, con el acompañamiento de la Oficina Asesora de Planeación y el respaldo de la Oficina de Control Interno, permitiendo una adopción articulada, coherente y alineada con los lineamientos institucionales. Este proceso ha contado con la participación de los líderes operativos de cada área y sus equipos de trabajo, cuyo rol ha sido fundamental para la adecuada implementación y efectividad de los controles establecidos, fortaleciendo de manera significativa la gestión institucional en este ámbito.

Como resultado del seguimiento realizado a los riesgos de seguridad de la información durante el tercer cuatrimestre de 2025, se concluye que la gestión adelantada ha contribuido a la continuidad operativa y al cumplimiento de los objetivos definidos, fortaleciendo la ejecución de las actividades críticas y aportando de manera directa al logro de los objetivos estratégicos de la Entidad en materia de seguridad de la información.

Adicionalmente, a partir de las mesas de trabajo realizadas con las áreas y procesos, y en atención al informe de seguimiento emitido por la Oficina de Control Interno (OCI) mediante radicado No. 3-2025-42443 “Informe de seguimiento a riesgos de seguridad de la información – segundo cuatrimestre de 2025”, se evidenció un avance significativo en la validación y atención de las observaciones formuladas, lo cual permitió una evaluación más precisa de la implementación y efectividad de los controles y facilitó la incorporación de las recomendaciones formuladas.

En concordancia con la Política de Administración de Riesgos, que establece la actualización de los activos de información como un componente fundamental para la gestión de los riesgos de seguridad de la información, durante el tercer cuatrimestre de la vigencia 2025 se realizó la actualización de los activos de información, de acuerdo con la programación definida de manera conjunta entre la Dirección de Recursos Físicos y Gestión Documental y la DTSI, fortaleciendo la identificación, valoración y control de los riesgos asociados.

Se resalta, asimismo, el compromiso de los Líderes de Proceso y Líderes Operativos, junto con sus equipos de trabajo, en la implementación y ejecución de los controles definidos. En este sentido, la DTSI extiende un reconocimiento especial a los colaboradores que garantizaron el cumplimiento oportuno de las actividades de seguimiento y el cargue adecuado de evidencias durante el tercer cuatrimestre de 2025, contribuyendo de manera significativa al fortalecimiento de la gestión institucional de la seguridad de la información.

Finalmente, la Dirección de Tecnologías y Sistemas de la Información, en el marco de su compromiso con la mejora continua, ratifica su disposición para brindar el acompañamiento metodológico requerido en la gestión de los riesgos de seguridad de la información, incluyendo la orientación técnica frente a eventuales ajustes en las caracterizaciones, procedimientos y documentos que soportan la gestión de los procesos, lo cual podrá derivar en la actualización de riesgos o controles, conforme a las necesidades institucionales y al marco normativo vigente.