ALCALDÍA MAYOR DE BOGOTÁ
SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA
AL RESPONDER CITAR EL NR.
Nro. Rad: 3-2025-19176
Fecha: 16/05/2025 10:32:49 AM
Destino: 130-OCI

MEMORANDO

Para: KAROL ANDREA PARRAGA HACHE
OFICINA DE CONTROL INTERNO

De: DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION

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

Respetada Doctora: Párraga.

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.: RAFAEL HUMBERTO LOPEZ SAAVEDRA-DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION
JORGE ELIECER VELASQUEZ PERILLA-DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION
EDWIN CASTILLO ORTIZ-DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION
FRANCISCO ALFORD BOJACA-COBRO PERSUASIVO
OSCAR ALBERTO PORRAS MURCIA-EQUIPO ATENCION AL CIUDADANO
JULIAN PONTON SILVA-OFICINA ASESORA DE PLANEACION
DAMIAN CAMILO VARGAS VARGAS-OFICINA ASESORA DE PLANEACION

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

PAOLA ANDREA CHACON TELLEZ-OFICINA ASESORA DE COMUNICACIONES
YESSICA PAOLA NOGUERA BECERRA-OFICINA ASESORA DE COMUNICACIONES
DIEGO ALEXANDER URAZAN FRANCO-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
EDITH NATHALIE ROMERO BARRERA-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
ESTEFANIA ESTRADA VILLADA-SUBSECRETARIA DE SEGURIDAD Y CONVIVENCIA
ALEJANDRO REYES LOZANO-DIRECCION DE PREVENCION Y CULTURA CIUDADANA
LINA MARIA TORO TAMAYO.-SUBSECRETARIA DE ACCESO A LA JUSTICIA
VIVIANA PAOLA RODRIGUEZ RODRIGUEZ-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
EFRAIN ARMANDO ZAMBRANO CAMARGO-DIRECCION DE RESPONSABILIDAD PENAL ADOLESCENTE
ORLANDO VEGA NAVAS-DIRECCION DE BIENES PARA LA SEGURIDAD, CONVIVENCIA Y ACCESO A LA JUSTICIA
REINALDO RUIZ SOLORZANO-SUBSECRETARIA DE GESTION INSTITUCIONAL
VILMA PATRICIA FERREIRA LUGO-DIRECCION DE GESTION HUMANA
PIEDAD CONSTANZA PARDO RODRIGUEZ-DIRECCION DE GESTION HUMANA
DEIDER MAURICIO MENGUAL PATERNINA-DIRECCION FINANCIERA
DEISY NATALIA VALENCIA GONZALEZ-DIRECCION FINANCIERA
CT (RP) ADRIANA PATRICIA HERNANDEZ MARIN-DIRECCION DEL CENTRO ESPECIAL DE RECLUSION
Anexos: -1

Elaboró: DIEGO MAURICIO USME GONZALEZ
Revisó: JAIRO ALONSO BOHORQUEZ BLANCO-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 PRIMER CUATRIMESTRE 2025

Contenido

INTRODUCCIÓN

De conformidad con lo estipulado en la Política de Administración de Riesgos de la Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ (PO-FI-02- Ver. 1), específicamente en el ítem 13 sobre Publicación, Seguimiento y Evaluación de los Riesgos, para los riesgos de seguridad de la información la segunda Línea de Defensa para este caso la Dirección de Tecnologías y Sistemas de la Información tiene la responsabilidad de realizar un seguimiento cuatrimestral a la Matriz de Riesgos y remitir el informe correspondiente a la Oficina de Control Interno dentro de los primeros 10 días hábiles posteriores al cierre del cuatrimestre. En este contexto, el presente informe expone las actividades desarrolladas durante el primer cuatrimestre de la vigencia 2025.

El seguimiento a la matriz de riesgos de seguridad de la información se fundamenta en el proceso previo de levantamiento de activos, en el cual se validaron 322 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, 154 con criticidad Media y 97con criticidad Baja.

A partir de los 71 activos clasificados con criticidad Alta, y conforme al proceso aprobado previamente mediante acta de reunión, se identificaron y estructuraron 28 riesgos asociados a la seguridad de la información, para los cuales se definieron un total de 36 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)
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 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. 1 adoptada por la SDSCJ. Dicha política está alineada con las directrices establecidas en la "Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 6 - noviembre de 2022" del Departamento Administrativo de la Función Pública – DAFP.

1. Conocimiento y Divulgación.

En el mes de abril 2025, la Dirección de Tecnologías y Sistemas de la Información (DTSI) llevó a cabo el diseño y la divulgación de una pieza gráfica titulada “Seguimiento de control de riesgos de seguridad de la información”, la cual fue difundida de manera masiva a toda la Entidad como parte de sus actividades de socialización. Las evidencias correspondientes están disponibles en el siguiente enlace:
https://scjgovcol.sharepoint.com/:f:/r/sites/DireccionTIC/Documentos%20compartidos/GobiernoTI/MIPG/Riesgos/Seguridad%20Informaci%C3%B3n/Informes/2025/Primer%20Cuatrimestre/Piezas%20Graficas?csf=1&web=1&e=gSh54m

Gráfica.1 Elaboración Uso y Apropiación DTSI.

Adicionalmente, la Dirección de Tecnologías y Sistemas de la Información (DTSI) emitió el memorando electrónico digital 3-2025-13744 del 08 de abril de 2025, en el cual se proporciona información sobre el cargue de evidencias relacionadas con los controles implementados para mitigar los riesgos de seguridad de la información correspondientes a los meses de enero, febrero, marzo y abril (primer cuatrimestre de la vigencia 2025), dirigido a los procesos y áreas previamente definidos. El enlace para acceder a dicha información es el siguiente:

https://scjgovcol.sharepoint.com/:b:/r/sites/DireccionTIC/Documentos%20compartidos/GobiernoTI/MIPG/Riesgos/Seguridad%20Informaci%C3%B3n/Informes/2025/Primer%20Cuatrimestre/Memorando/3-2025-13744.pdf?csf=1&web=1&e=U7NOqv

Igualmente, se llevó a cabo la difusión de la información mediante correo electrónico dirigido a todas las áreas responsables de la gestión de riesgos de seguridad de la información. En dicha comunicación se incluyó orientación sobre el cargue de evidencias correspondiente al primer cuatrimestre, así como la validación de las observaciones realizadas por la Oficina de Control Interno respecto al informe de riesgos de seguridad de la información del tercer cuatrimestre de 2024. 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/Informes/2025/Primer%20Cuatrimestre/Comunicaciones%20Electronicas?csf=1&web=1&e=E8MjS4

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

En el transcurso del primer cuatrimestre de 2025, personal de la Dirección de Tecnologías y Sistemas de la Información (DTSI) participó en la mesa técnica de gobierno y seguridad digital, presentando las actividades realizadas sobre la actualización de activos de información, el cargue de dichos activos en la plataforma de Datos Abiertos Bogotá y en el sitio web institucional de la Entidad.

La Dirección de Recursos Físicos y Gestión Documental, en coordinación con la Dirección de Tecnologías y Sistemas de la Información, llevó a cabo mesas de trabajo con el proceso de Gestión de Emergencias para la revisión, ajuste y actualización de los activos de información, en atención a la incorporación de nuevos activos asociados a dicho proceso. Asimismo, con el proceso de Gestión Documental se realizó mesa de trabajo enfocada en la actualización del borrador del formato F-GD-1081 – Registro de Activos de Información e Índice de Información Clasificada y Reservada, para su trámite y aprobación ante la Oficina Asesora de Planeación, y posterior cargue en el Portal MIPG de la Entidad. Los avances relacionados con la actualización de activos de información se encuentran consolidados en el siguiente enlace:

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

Con base en la información anterior, se puede confirmar que la actualización del Registro de Activos de Información y del Índice de Información Clasificada y Reservada ha sido publicada en el sitio web institucional de la Entidad, disponible en el siguiente enlace:

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

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-es-transparencia-datos-abiertos-registros-activos-informacion.

3. Identificación del riesgo.

Para el primer cuatrimestre del 2025, se dio gestión 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:

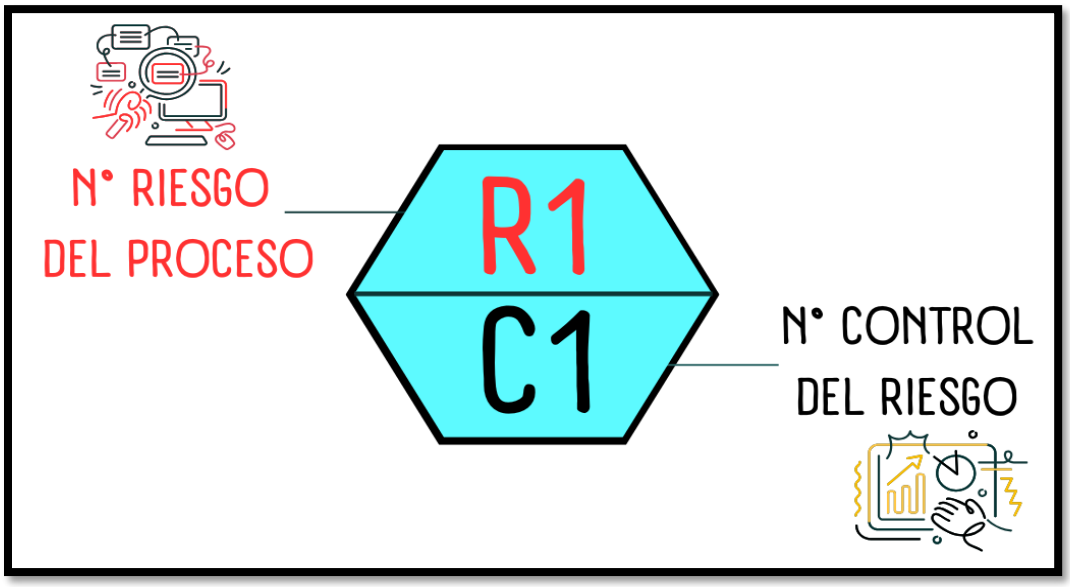
- **WEB**: https://scj.gov.co/es Transparencia y Acceso a la información pública - Planeación, políticas lineamientos y manuales -Plan de acción - Matriz de riesgos Seguridad de la Información – 2025.
  https://scj.gov.co/es/transparencia/planeacion-presupuesto-ingresos/plan-accion

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

- Se cuenta con una (1) Matriz General de riesgos de seguridad de la información con la agrupación de la información de los Riesgos de todos los procesos con la información de la Hoja de resumen, listado de activos, Riesgo Inherente, Tratamiento del Riesgo, Valoración con controles y Tratamiento de riesgo residual.

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

- La nomenclatura asignada a cada riesgo corresponde a lo siguiente:



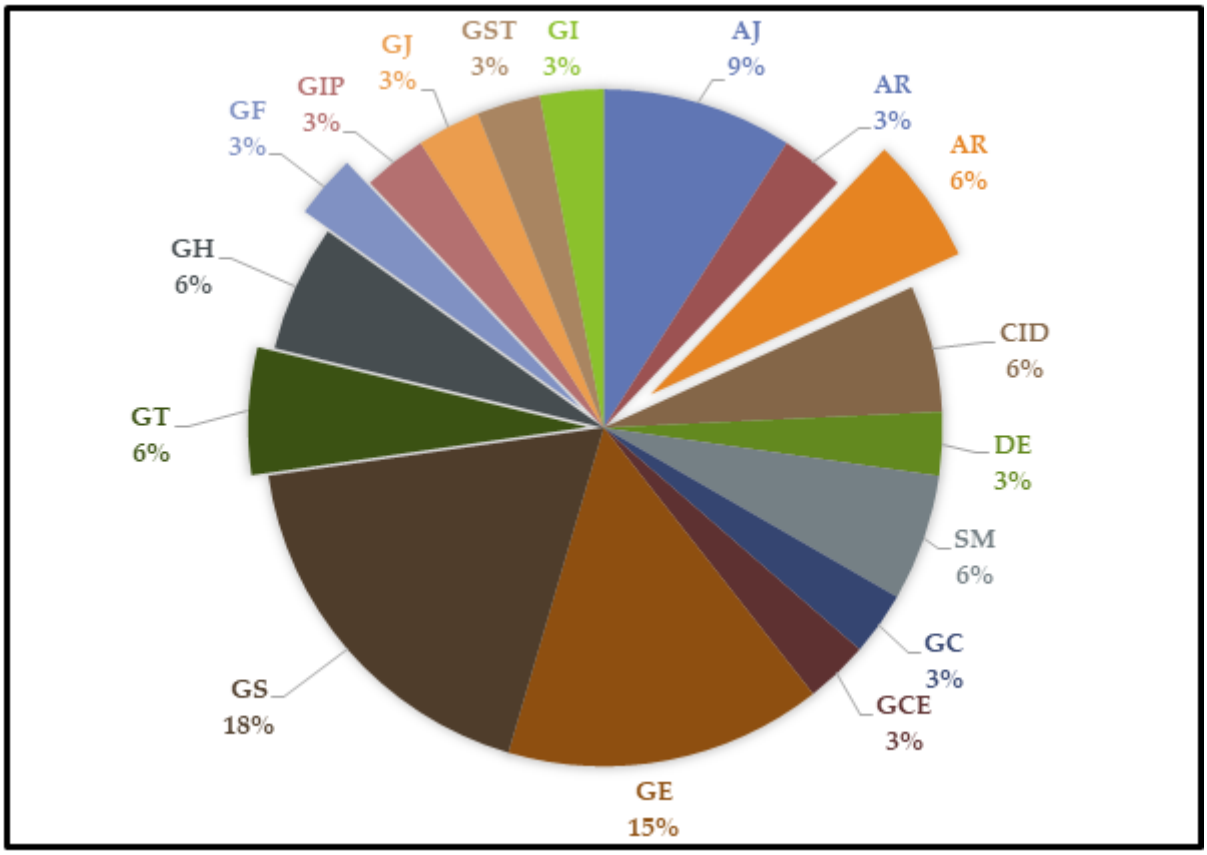
Grafica 2. Nomenclatura Riesgos.

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

PROCESO	SIGLA	RIESGOS
Acceso y Fortalecimiento a la Justicia	AJ	3
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	1
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	6
Gestión de Tecnología de Información	GT	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	33

Tabla 2. Procesos Riesgos de Seguridad de Información.

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%

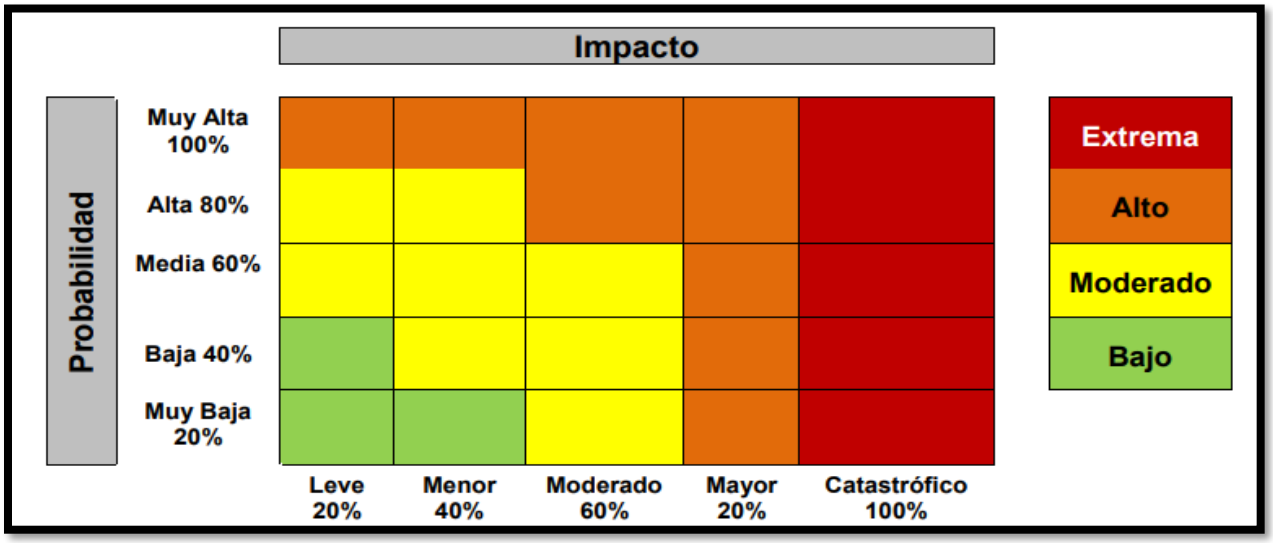
Grafica 4. Fuente: Política de Administración de Riesgos SDSCJ.

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)			2	1	3
Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas. (AB)			4		4
Atención y Relación con el Ciudadano (AR)			2		2
Control Disciplinario (CID)			2		2
Direccionamiento Estratégico. (DE)		1			1
Evaluación al Sistema de Control Interno (SM)			3		3
Gestión Contractual (GC)			1		1
Gestión de Comunicaciones Estratégicas. (GCE)			1		1
Gestión de Emergencias (GE)			7		7
Gestión de Seguridad y Convivencia (GS)			7		7
Gestión de Tecnología de Información (GT)		4			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)			2		2
Gestión y Análisis de Información (GI)		1			1
Total	**0**	**6**	**36**	**1**	**43**

Tabla 3. Valoración Riesgos SDSCJ

Considerando la necesidad de garantizar la continuidad y ejecución de los procedimientos definidos por los procesos, no se adoptó la opción de “Evitar” como medida de tratamiento para ninguno de los riesgos identificados. Por el contrario, los procesos optaron por la medida de “Reducir el riesgo”, lo que implica la implementación de controles orientados a minimizar la probabilidad de ocurrencia de dichos riesgos, en concordancia con los lineamientos establecidos 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 aclarar que el número de controles no guarda una relación directa con la materialización del riesgo. Estos controles han sido definidos por cada proceso con base en su criterio y recursos disponibles, con el propósito de prevenir, en la medida de lo posible, la ocurrencia de dichos riesgos.

Proceso	N° Riesgos	N° Controles
Acceso y Fortalecimiento a la Justicia (AJ)	3	3
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)	1	1
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)	**6**	**7**
Gestión de Tecnología de Información (GT)	**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**	**1**
Total	**33**	**43**

Tabla 4. Riesgos y Controles

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 trimestralmente solicita la verificación de los permisos de derecho de acceso a los diferentes formularios, de acuerdo con los roles y responsabilidades asignados para tal fin, como soporte de la revisión enviará este profesional comunicación oficial y/o correo electrónico a los responsables del área solicitando esta información, en caso que los usuarios no tengan autorización se retiraran permisos de acceso y se informara de las acciones al Jefe de área.
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	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 se debe informar al director de Bienes con las acciones para dar cumplimiento.
R4-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.
R4-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 a las funcionalidades y servicios, como soporte de la evidencia se dejará las listas de asistencia y/o soportes documentales de las capacitaciones, para los casos que el personal no asista se reprogramará una nueva sesión de capacitación
R4-C4	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	Pérdida de la Integridad	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
R5-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.
R6-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.
R7-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.
R8-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.
R9-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.

R10-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.
R10-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.
R11-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.
R12-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.
R13-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.
R14-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.
R14-C2	Gestión de Emergencias	Pérdida de la Integridad	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.
R14-C3	Gestión de Emergencias	Pérdida de la Disponibilidad	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.
R15-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.
R16-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.
R17-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.
R18-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.
R19-C1	Gestión de Seguridad y Convivencia	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.
R20-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.
R20-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.
R21-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.
R22-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.
R23-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.
R24-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.
R25-C1	Gestión de Tecnología de Información	Pérdida de Confidencialidad, integridad y/o disponibilidad de la información	El responsable de sistema de información y/o infraestructura Tecnológica verifica de forma cuatrimestral el seguimiento al plan de trabajo de versionamiento de los ambientes de pruebas y productivos asociados a los sistemas de información, en caso de no realizar el seguimiento se debe evidenciar las causas de no realizar las actividades del plan a través de actas, informes y/o correos electrónicos, como evidencia de la ejecución del control se contara con los avances de las actividades del plan mediante bitácoras de actividades, actas y/o comunicado oficial.
R25-C2	Gestión de Tecnología de Información	Pérdida de Confidencialidad, integridad y/o disponibilidad de la información	El responsable de sistema de información realiza seguimiento cuatrimestral a la ejecución del plan de actualización documental de la arquitectura de los sistemas de información, en caso de no contar con el seguimiento trimestral al plan de actualización documental de la arquitectura, se deberá contar con los manuales técnicos actualizados de cada uno de los sistemas de información. Como evidencia de la ejecución del control se contará con el reporte de seguimiento al plan o con los manuales técnicos de los sistemas
R26-C1	Gestión de Tecnología de Información	Pérdida de Confidencialidad, integridad y/o disponibilidad de la información	El responsable de infraestructura define el mecanismo seguro y estandarizado para la gestión segura de credenciales de administración en la infraestructura tecnológica, así como el seguimiento trimestral al cumplimiento de los mecanismos establecidos, en caso de no contar con el seguimiento trimestral a los mecanismos establecidos, se contará con comunicación formal al Director de Tecnologías informando las alternativas adoptadas. Como evidencia de la ejecución del control se contará con el mecanismo de gestión segura de contraseñas o comunicado formal.
R26-C2	Gestión de Tecnología de Información	Pérdida de Confidencialidad, integridad y/o disponibilidad de la información	El responsable de infraestructura tecnológica realiza seguimiento trimestral al funcionamiento de herramientas de seguridad informática que protegen la información de la SDSCJ, en caso de no hacer seguimiento al funcionamiento se contara con comunicación formal al Director de Tecnologías informando las alternativas adoptadas. Como evidencia de la ejecución del control se contará con el reporte de rendimiento de la infraestructura de seguridad o el comunicado formal.
R27-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.
R28-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.

R29-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.
R30-C1	Gestión Integral a las Personas Privadas de la Libertad - PPL.	Pérdida de la Disponibilidad Perdida de Confidencialidad	El Secretario del Centro Especial de Reclusión, registra y valida cuando se requiera las solicitudes de acceso a información archivada, validando previamente que las mismas hayan sido autorizadas por la Dirección del C.E.R a través de memorando y/o correo electrónico; a su vez tendrá a su cargo las llaves del archivador de documentos ubicado en el área administrativa del Centro, en caso de no contar con solicitud o requerimiento previo se debe solicitar esta autorización a la dirección del CER, una vez sea autorizada, se debe dejar este soporte para efectos de trazabilidad, la evidencia se reportara de forma Cuatrimestral.
R31-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.
R32-C1	Gestión Tecnológica de Seguridad y Emergencias.	Pérdida de Confidencialidad, Integridad y/o disponibilidad de la información	El supervisor del contrato de mantenimiento de video vigilancia y los profesionales de apoyo al mismo, realizan seguimiento a los mantenimientos de los equipos que conforman el sistema de video vigilancia, como evidencia se debe presentar el reporte mensual de los mantenimientos realizados avalado por la interventoría y/o supervisión acompañado de la conciliación técnica mensual de ANS aplicados al contratista, mes vencido, en caso de no contar con los reportes que entrega el contratista, se realizaran las gestiones pertinentes mediante comunicado oficial y/o correo electrónico sobre la información. El cargue de las evidencias se consolidará de forma cuatrimestral.
R32-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.
R33-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.

Tabla 5. Estructuración de Controles.

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.

6. Tratamiento del Riesgo Residual.

Desde la Dirección de Tecnologías y Sistemas de la Información (DTSI) se brindó acompañamiento permanente a todos los procesos de la Entidad, con el fin de facilitar el cumplimiento de los parámetros establecidos en materia de gestión de riesgos de seguridad de la información. Este apoyo se tradujo en orientación técnica, articulación interprocesos y seguimiento al cumplimiento de las actividades requeridas, lo cual permitió alcanzar un cumplimiento integral de los controles definidos.

Gracias a este trabajo articulado, se logró una adecuada implementación de las medidas de tratamiento del riesgo, lo que contribuye significativamente a la mitigación de las amenazas identificadas y a una apropiada gestión institucional del riesgo.

Los resultados de dicha gestión pueden evidenciarse mediante el análisis comparativo entre la Zona de Riesgo Inherente y la Zona de Riesgo Residual, lo cual se detalla en el siguiente cuadro, permitiendo observar la efectividad de los controles ejecutados por cada proceso.

PROCESO	INHERENTE				RESIDUAL			
	EXTREMO	ALTO	MODERADO	BAJA	EXTREMO	ALTO	MODERADO	BAJA
Acceso y Fortalecimiento a la Justicia (AJ)			2	1				3
Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas. (AB)			4					4
Atención y Relación con el Ciudadano (AR)			2					2
Control Disciplinario (CID)			2					2
Direccionamiento Estratégico. (DE)		1						1
Evaluación al Sistema de Control Interno (SM)			3					3
Gestión Contractual (GC)			1					1
Gestión de Comunicaciones Estratégicas. (GCE)			1					1
Gestión de Emergencias (GE)			7					7
Gestión de Seguridad y Convivencia (GS)			7					7
Gestión de Tecnología de Información (GT)		4						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)			2					2
Gestión y Análisis de Información (GI)		1						1
Total	**0**	**6**	**36**	**1**	**0**	**0**	**0**	**43**

Tabla 6. Zona de Riesgo Inherente y Zona de Riesgo Residual

7. Monitoreo, revisión y reporte.

Recomendaciones OCI.

En atención a las conclusiones y recomendaciones emitidas por la Oficina de Control Interno (OCI) a través del memorando # 3-2025-7706, correspondiente al "Informe de seguimiento a riesgos de seguridad de la información - tercer cuatrimestre de 2024", se llevaron a cabo mesas de trabajo con las áreas involucradas, con el fin de validar las observaciones realizadas por la OCI respecto a la evaluación de los controles y las evidencias presentadas:

7.1 Proceso Acceso y Fortalecimiento a la Justicia (AJ).

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

Para esta recomendación, se informó por parte del equipo de trabajo del proceso Acceso y Fortalecimiento a la Justicia (AJ), que se realizará el cargue de las evidencias solicitadas por la OCI, y ajustes correspondientes el control, así:

Atención a recomendación:

Control Actual:

Los responsables de la generación de información (funcionarios públicos y/o contratistas) verifican de forma cuatrimestral la entrega de soportes relacionados con el cumplimiento de metas relacionadas al Plan de Acceso a la Justicia de acuerdo con la naturaleza de los documentos (mensual - trimestral -semestral y anual) a la Dirección de Acceso a la Justicia. En caso de incumplimiento de la entrega de los documentos en los plazos establecidos, el Director o su equipo delegado de DAJ solicita a los responsables la entrega oportuna de la información, sopena del incumplimiento de metas, requerimientos internos y externos; como evidencia se entrega los soportes de la documentación entregada en los repositorios SharePoint disponibles para el área.

De acuerdo con las revisiones y análisis del control se propone por parte del grupo estructurador con el apoyo de la DTSI, los siguientes ajustes, así:

Proyección y ajustes del control:

Se realiza ajustes sobre el activo de acuerdo con la actualización de activos de información vigencia 2024:

Activo: "Registros DAJ (Registros de orientaciones y atenciones en Centros de Recepción e Información de Casas de Justicia, Registros de orientaciones y atenciones en Unidades Móviles de Acceso a la Justicia, Registros de orientaciones en canales no presenciales de Casas de Justicia, Registros de orientaciones y atenciones en Unidades de Mediación y Conciliación, Registros de orientaciones de la estrategia de facilitadores de acceso a la justicia)"

Amenaza: Abuso de Derechos.

Vulnerabilidad: Asignación errada de los derechos de acceso.

RIESGO #	PROCESO	ACTIVO	TIPO DE ACTIVO	RIESGO	AMENAZA	VULNERABILIDAD
1	Acceso y Fortalecimiento a la Justicia.	Registros DAJ (Registros de orientaciones y atenciones en Centros de Recepción e Información de Casas de Justicia. Registros de orientaciones y atenciones en Unidades Móviles de Acceso a la Justicia. Registros de orientaciones en canales no presenciales de Casas de Justicia. Registros de orientaciones y atenciones en Unidades de Mediación y Conciliación. Registros de orientaciones de la estrategia de facilitadores de acceso a la justicia)	Información	Pérdida de la Integridad	Abuso de derechos.	Asignación errada de los derechos de acceso.

Grafica 7. Ajuste y recomendación Riesgo R1-C1

Ajuste Control:

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.

Asignación errada de los derechos de acceso.	Pérdida o detrimento de información	Los responsables de la generación de información (funcionarios públicos y/o contratistas) verifican de forma cuatrimestral la entrega de soportes relacionados con el cumplimiento de metas relacionadas al Plan de Acceso a la Justicia de acuerdo con la naturaleza de los documentos (mensual - trimestral -semestral y anual) a la Dirección de Acceso a la Justicia. En caso de incumplimiento de la entrega de los documentos en los plazos establecidos, el Director o su equipo delegado de DAJ solicita a los responsables la entrega oportuna de la información, sopena del incumplimiento de metas, requerimientos internos y externos; como evidencia se entrega los soportes de la documentación entregada en los repositorios SharePoint disponibles para el área.	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.

Grafica 8. Ajuste y recomendación Riesgo 1 - Control 1

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

  Para esta recomendación, se informó por parte del equipo de trabajo del proceso Acceso y Fortalecimiento a la Justicia (AJ), que se realizará el cargue de las evidencias solicitadas por la OCI, y ajustes correspondientes el control, así:

  Atención a recomendación:

Control Actual:

El profesional y/o los profesionales de la dirección de acceso designados para esta actividad trimestralmente solicita la verificación de los permisos de derecho de acceso a los diferentes formularios, de acuerdo con los roles y responsabilidades asignados para tal fin, como soporte de la revisión enviará este profesional comunicación oficial y/o correo electrónico a los

responsables del área solicitando esta información, en caso que los usuarios no tengan autorización se retiraran permisos de acceso y se informara de las acciones al Jefe de área.

De acuerdo con las revisiones y análisis del control se propone por parte del grupo estructurador con el apoyo de la DTSI, los siguientes ajustes, así:

Proyección y ajustes del control:

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.

da de los derechos de cceso.	Pérdida o detrimento de información	El profesional y/o los profesionales de la dirección de acceso designados para esta actividad trimestralmente solicita la verificación de los permisos de derecho de acceso a los diferentes formularios, de acuerdo con los roles y responsabilidades asignados para tal fin, como soporte de la revisión enviará este profesional comunicación oficial y/o correo electrónico a los responsables del área solicitando esta información, en caso que los usuarios no tengan autorización se retiraran permisos de acceso y se informara de las acciones al Jefe de área.	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.

Grafica 9. Ajuste y recomendación R2–C1

7.2 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.

Para esta recomendación, por parte del grupo estructurador proceso Administración De Bienes Muebles E Inmuebles Para El Fortalecimiento De Las Capacidades Operativas (AB), se informa que en el próximo cumplimiento del primer cuatrimestre de riesgos de seguridad de Información 2025 se presentaran las evidencias del cargue del control de acuerdo con las recomendaciones de la OCI.

- Recomendación riesgo 4 – control 2: Revisión y ajustes de evidencias.

Para esta recomendación, por parte del grupo estructurador proceso Administración De Bienes Muebles E Inmuebles Para El Fortalecimiento De Las Capacidades Operativas (AB), se informa que en el próximo cumplimiento del primer cuatrimestre de riesgos de seguridad de Información 2025 se presentaran las evidencias del cargue del control de acuerdo con las recomendaciones de la OCI.

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

Para esta recomendación, por parte del grupo estructurador proceso Administración De Bienes Muebles E Inmuebles Para El Fortalecimiento De Las Capacidades Operativas

(AB), se informa que en el próximo cumplimiento del primer cuatrimestre de riesgos de seguridad de Información 2025 se presentaran las evidencias del cargue del control de acuerdo con las recomendaciones de la OCI.

7.3 Proceso Atención y relación con el Ciudadano (AR).

- ❖ Recomendación riesgo 6 – control 1: Revisión y ajustes de evidencias.

Para esta recomendación, se informa por parte del equipo de trabajo del proceso Atención y Relación al Ciudadano (AR) que se cargó la evidencia referente al tercer cuatrimestre de la vigencia 2024 correspondiente, así mismo se reitera que en el próximo cumplimiento para el seguimiento del primer cuatrimestre de riesgos de seguridad de Información vigencia 2025 se presentara de acuerdo con las recomendaciones de la OCI.

Gráfica.10 Ajuste y recomendación R2–C1

7.4 Proceso Direccionamiento Estratégico (DE).

- ❖ Recomendación riesgo 9 - control 1: Revisión y ajustes de evidencias.

Para esta recomendación, se informa por parte del equipo de trabajo del proceso Direccionamiento Estratégico (DE) que en el próximo cumplimiento para el seguimiento del primer cuatrimestre de riesgos de seguridad de Información vigencia 2025 se presentara de acuerdo con las recomendaciones de la OCI.

7.5 Proceso de Gestión de Emergencias (GE).

- ❖ Recomendación riesgo 14 - control 1: Revisión y ajustes de evidencias.

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.

Grafica 11. Cargue Evidencias R14–C1

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

Para esta recomendación, se informa por parte del equipo de trabajo del proceso de Gestión de Emergencias (GE), se realizarán consultas internas sobre la validación y/o actualización del control de acuerdo con las recomendaciones generadas.

Dentro de las evidencias presentadas se establece para el primer cuatrimestre de riesgos de seguridad de Información se presentará de acuerdo con las recomendaciones de la OCI.

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

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

- Recomendación riesgo 18 - control 1: Revisión y ajustes de evidencias.

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

7.6 Proceso Gestión de Seguridad y Convivencia (GS).

- Recomendación riesgo 23 – control 1: Revisión y ajustes de evidencias.

De acuerdo con las revisiones y análisis del control se propone por parte del grupo estructurador con el apoyo de la DTSI, una revisión detallada del activo, para intentar mitigar las situaciones que ha indicado la OCI desde el mismo momento en que se realicen los registros y que esto podrá implicar un eventual ajuste del control.

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

- Recomendación riesgo 24 – control 1: Ajustar Control.

Para esta recomendación, se informó por parte del equipo de trabajo del proceso Gestión de Seguridad y Convivencia (GS), que, de acuerdo con las recomendaciones de la OCI, se realizarán ajustes al control, así:

Control inicial:

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 mediante la tabla de verificación de correspondencia 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.

De acuerdo con las revisiones y análisis del control se propone por parte del grupo estructurador con el apoyo de la DTSI, la estructura del control:

Control Ajustado:

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.

Pérdida o detrimento de información Perdida de confianza del ciudadano Demandas, litigios, derechos de petición o tutelas	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 mediante la tabla de verificación de correspondencia 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.	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.

Gráfica.12. Cargue Evidencias R24–C1

7.7 Proceso Gestión de Tecnología de Información (GT)

- Recomendación riesgo 25 - control 1: Ajustar Evidencias.

Para esta recomendación, por parte del grupo de sistemas de información de la Dirección de Tecnologías y Sistemas de la Información se informó que para el primer cuatrimestre de riesgos de seguridad de Información se presentarán las evidencias del cargue del control de acuerdo con las recomendaciones de la OCI.

- Recomendación riesgo 25 - control 2: Ajustar Evidencias.

Para esta recomendación, por parte del grupo de sistemas de información de la Dirección de Tecnologías y Sistemas de la Información se informa que en el próximo cumplimiento del primer cuatrimestre de riesgos de seguridad de Información 2024 se presentarán las evidencias del cargue del control de acuerdo con las recomendaciones de la OCI.

- Recomendación riesgo 26 – control 1: Ajustar Control.

Para esta recomendación, por parte del grupo de Infraestructura Tecnológica de la Dirección de Tecnologías y Sistemas de la Información, se realizará mesas de trabajo internas para atender las recomendaciones provistas de la OCI para el cierre del tercer cuatrimestre 2024 y se informa que para el segundo cuatrimestre de riesgos de seguridad de Información 2024 se establecerán las mesas de trabajo respectivas al interior de la DTSI, para publicar el documento de Gestión segura de contraseñas.

7.8 Gestión Estratégica del Talento Humano (GH)

- Recomendación riesgo 27 - control 1: Ajustar Evidencias.

Para esta recomendación, se informó por parte del equipo de trabajo de la oficina de la Dirección de Tecnologías y Sistemas de la Información que se realizó los ajustes necesarios en los títulos y la codificación de los repositorios SharePoint para el cargue de evidencias del proceso Gestión Estratégica del Talento Humano (GH), así como para los demás repositorios de todas las áreas y procesos de la Entidad.

Grafica 13. Ajuste recomendación R27–C1

Grafica 14. Ajuste recomendación R28–C1

7.9 Proceso Financiera (GF).

- ❖ Recomendación riesgo 29 - control 1: Ajustar Control.

Para esta recomendación, por parte del grupo estructurador de la Dirección Financiera, se informa que en el próximo cumplimiento del primer cuatrimestre de riesgos de seguridad de Información 2025 se presentaran las evidencias del cargue del control de acuerdo con las recomendaciones de la OCI.

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

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

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

Para esta recomendación, se informa por parte del equipo de trabajo del proceso de Gestión de Emergencias (GE), se realizarán consultas internas sobre la validación y/o actualización del control de acuerdo con las recomendaciones generadas.

Dentro de las evidencias presentadas se establece para el primer cuatrimestre de riesgos de seguridad de Información se presentará de acuerdo con las recomendaciones de la OCI.

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

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 primer cuatrimestre de riesgos de seguridad de Información se entregara de acuerdo con las recomendaciones de la OCI.

- ❖ Recomendación riesgo 32 - control 2: Revisión y ajustes de evidencias.

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 primer cuatrimestre de riesgos de seguridad de Información se entregara de acuerdo con las recomendaciones de la OCI.

7.11 Gestión y Análisis de Información (GI).

- ❖ Recomendación riesgo 33 - control 1: Revisión y ajustes de evidencias.

Para esta recomendación, por parte del grupo estructurador del proceso Gestión y Análisis de Información (GI), se informa que se cargó la evidencia correspondiente al tercer cuatrimestre de acuerdo con las recomendaciones establecidas y adicionalmente en el próximo cumplimiento del primer cuatrimestre de riesgos de seguridad de Información 2025 se presentarán las evidencias del cargue del control de acuerdo con las recomendaciones de la OCI.

Grafica 15. Ajuste Cargue Evidencias R33–C1

La Dirección de Tecnologías y Sistemas de la Información se permite realizar las siguientes aclaraciones con base a los controles establecidos y las evidencias suministradas:

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, fueron documentadas mediante la elaboración de sus respectivas actas. Estas actas 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/Informes/2025/Primer%20Cuatrimestre/Mesas%20de%20Trabajo?csf=1&web=1&e=LHmH8x

❖ **Oportunidad de Mejora 1.**

En atención a la oportunidad de mejora identificada, se adelantó mesa de trabajo con el personal de la Dirección de Recursos Físicos y Gestión Documental (DRFGD), Durante la sesión se establecieron diversas consideraciones, destacándose como prioridad la necesidad de robustecer los controles establecidos para la gestión de riesgos por proceso. Asimismo, se enfatizó la importancia de crear y formalizar riesgos y controles específicos asociados a la seguridad de la información.

En este sentido, se programarán para el segundo cuatrimestre de la vigencia 2025, las mesas de trabajo orientadas a:

- La actualización y categorización de los activos de información de la DRFGD.
- La identificación, análisis y documentación de los riesgos de seguridad de la información correspondientes.

❖ **Oportunidad de Mejora 2.**

En atención a la observación relacionada con la falta de concordancia entre los activos de información consignados en el Formato F-GD-1081 “Registro de Activos de Información” y aquellos registrados en la matriz de riesgos de seguridad de la información (F-FI-1385), se informa que ya se realizaron los ajustes correspondientes.

Se llevó a cabo una revisión y actualización de los activos de información vinculados al proceso "Acceso y Fortalecimiento a la Justicia", garantizando la consistencia entre la hoja “Listado De Activos” y la hoja “Riesgo Inherente” de la matriz. Actualmente, ambos listados presentan concordancia en cuanto a los ítems y descripciones, en cumplimiento con la metodología institucional.

Adicionalmente, se realizó la incorporación de las amenazas identificadas en la matriz F-FI-1385 que no estaban previamente catalogadas en el borrador de la actualización de la G-FI-04: Guía de Administración del Riesgos presentada a la oficina asesora de planeación para la actualización documental en el Portal MIPG.

❖ **Oportunidad de Mejora 3.**

Ante la Oficina Asesora de Planeación se realizó la presentación correspondiente al ajuste y actualización de los siguientes documentos:

- PO-FI-02: Política de Administración de Riesgos.
- G-FI-04: Guía de Administración del Riesgos.
- F-FI-1385: Matriz de Riesgos de Seguridad de la Información.

Durante el proceso de revisión, se identificó una serie de amenazas relacionadas con la seguridad de la información que no estaban previamente contempladas en la guía institucional para la administración de riesgos (G-FI-04). Esta guía establece las

directrices claras y detalladas sobre la implementación, operación, mantenimiento y mejora del Sistema Integrado de Gestión de la Entidad.

- **Oportunidad de Mejora 4.**

  En atención a la recomendación relacionada con la falta de inclusión de tipologías de controles automáticos y manuales en la matriz de riesgos de seguridad de la información, se informa que se programarán para el segundo y tercer cuatrimestre de la vigencia 2025, las respectivas mesas de trabajo con las áreas responsables de los procesos, con el fin de:

  - Revisar los controles existentes en la matriz F-FI-1385.
  - Clasificarlos adecuadamente según su tipología (automáticos o manuales).
  - Ajustar o incorporar nuevos controles conforme a los riesgos identificados.

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/Informes/2025/Primer%20Cuatrimestre/Oportunidad%20de%20Mejora?csf=1&web=1&e=NIrVMR

8. CARGUE EVIDENCIAS

A través del memorando interno No. 3-2025-13744 del 08 de abril de 2025, emitido por la Dirección de Tecnologías y Sistemas de la Información (DTSI), se solicitó el cargue de información correspondiente al primer cuatrimestre de la vigencia 2025. Esta solicitud se fundamentó en las recomendaciones del informe de seguimiento a los controles asociados a los riesgos de seguridad de la información del tercer cuatrimestre de 2024, elaborado por la Oficina de Control Interno. En dicho memorando se proporcionaron orientaciones sobre los ajustes requeridos en la entrega de evidencias por parte de los procesos y áreas para la actual vigencia.

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?csf=1&web=1&e=vl5297

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

Sigla	Proceso	N° Riesgos	N° Controles	Evidencias publicadas controles	% de riesgos cubierto
AJ	Acceso y Fortalecimiento a la Justicia	**3**	**3**	15	100%
AB	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	**1**	**4**	20	100%
AR	Atención y Relación con el Ciudadano	**2**	**2**	15	100%
CID	Control Disciplinario	**2**	**2**	4	100%
DE	Direccionamiento Estratégico.	**1**	**1**	11	100%
SM	Evaluación al Sistema de Control Interno	**2**	**3**	7	100%
GC	Gestión Contractual	**1**	**1**	1	100%
GCE	Gestión de Comunicaciones Estratégicas.	**1**	**1**	2	100%
GE	Gestión de Emergencias	**5**	**7**	31	100%
GS	Gestión de Seguridad y Convivencia	**6**	**7**	11	100%
GT	Gestión de Tecnología de Información	**2**	**4**	33	100%
GH	Gestión Estratégica del Talento Humano	**2**	**2**	4	100%
GF	Gestión Financiera.	**1**	**1**	4	100%
GIP	Gestión Integral a las Personas Privadas de la Libertad - PPL.	**1**	**1**	1	100%
GJ	Gestión Jurídica	**1**	**1**	1	100%
GST	Gestión Tecnológica de Seguridad y Emergencias.	**1**	**2**	10	100%
GI	Gestión y Análisis de Información	**1**	**1**	5	100%
	Total	**33**	**43**	175	**100%**

Tabla 7. 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 primer cuatrimestre del año 2025, la Dirección de Tecnologías y Sistemas de la Información ratifica su compromiso institucional mediante la revisión, actualización y seguimiento continuo a la matriz de seguridad de la información. Esta labor se desarrolla en cumplimiento de la Política de Administración de Riesgos y en alineación con los lineamientos establecidos por la *Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – Versión 6 (noviembre de 2022)* del Departamento Administrativo de la Función Pública (DAFP), contando con el respaldo permanente de los líderes operativos de cada proceso, quienes han desempeñado un papel clave en la implementación efectiva de los controles definidos.

Como resultado del seguimiento realizado durante el primer cuatrimestre del 2025 a los riesgos de seguridad de la información identificados por los procesos mencionados, se puede concluir que la gestión de estos riesgos ha favorecido la continuidad operativa, así como el cumplimiento de los objetivos establecidos. Este enfoque ha contribuido al fortalecimiento de la ejecución de actividades clave, impulsando el cumplimiento de los objetivos estratégicos de la Entidad en el ámbito de la seguridad de la información.

Como resultado de las mesas de trabajo desarrolladas con las áreas responsables, en atención al informe de seguimiento emitido por la Oficina de Control Interno (OCI) mediante el radicado 3-2025-7706 "*Informe de seguimiento a riesgos de seguridad de seguridad de la información - tercer cuatrimestre de 2024",* se ha evidenciado un avance significativo en la validación de las observaciones formuladas. Estas actividades han permitido una evaluación más precisa de los controles implementados. Asimismo, se resalta el compromiso y la activa participación de las áreas involucradas, quienes han contribuido de manera decidida en la implementación de las recomendaciones, fortaleciendo la efectividad de los controles establecidos.

En referencia a la actualización de los activos de información, establecida en la Política de Administración de Riesgos de la Entidad como un componente fundamental en la identificación, valoración, asignación, control y seguimiento de los riesgos de seguridad de la información que puedan afectar el desarrollo de los procesos y, por ende, el cumplimiento de los objetivos estratégicos, se llevó a cabo el inicio de las mesas de trabajo con las áreas para la actualización del registro de activos de información e índice de información clasificada y reservada para la vigencia 2025.

Es fundamental resaltar que la implementación de la Política de Administración de Riesgos en materia de seguridad de la información ha sido liderada por la Dirección de Tecnologías y Sistemas de la Información, con el acompañamiento de la Oficina Asesora de Planeación y el respaldo de la Oficina de Control Interno. Este ejercicio ha contado con la activa participación de los líderes operativos de cada proceso, lo cual ha permitido que la política se desarrolle y

adopte de manera articulada y coherente en el transcurso de la presente vigencia dentro de la Entidad.

Se destaca el compromiso demostrado por los Líderes de Proceso y Líderes Operativos, junto con sus respectivos equipos de trabajo, en la implementación y ejecución efectiva de los controles establecidos para la gestión de los riesgos de seguridad de la información. En ese sentido, desde la Dirección de Tecnologías y Sistemas de la Información se expresa un reconocimiento especial a todos los colaboradores que hicieron posible el cumplimiento oportuno de las actividades de seguimiento y cargue de evidencias durante el primer cuatrimestre del año 2025, contribuyendo significativamente al fortalecimiento de la gestión institucional en esta materia.

La Dirección de Tecnologías y Sistemas de la Información, en el marco de su compromiso con la mejora continua, reitera su responsabilidad y disposición para brindar el acompañamiento metodológico necesario en el ejercicio de gestión de riesgos de seguridad de la información correspondiente a la vigencia 2025. Este apoyo incluye la orientación ante eventuales ajustes o modificaciones en las caracterizaciones, procedimientos y documentación que respalden la gestión de cada proceso, y que puedan derivar en la actualización de riesgos o controles previamente identificados.

La Dirección de Tecnologías y Sistemas de la Información, en su mejora continua, para el ejercicio sobre la gestión de Riesgos de seguridad para la vigencia 2025 de la información, reitera su responsabilidad y compromiso en el apoyo metodológico requerido ante las posibles modificaciones o ajustes de las caracterizaciones, procedimientos y documentación que respalde la gestión de cada proceso y que conlleven al potencial cambio de riesgos o controles actualmente identificados.