ALCALDÍA MAYOR DE BOGOTÁ
SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA
AL RESPONDER CITAR EL NR.
Nro. Rad: 3-2025-36876
Fecha: 12/09/2025 03:22:34 PM
Destino: 130-OCI

MEMORANDO

Para: KAROL ANDREA PARRAGA HACHE
OFICINA DE CONTROL INTERNO

De: DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION

Asunto: INFORME SEGUNDO 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
EDWIN CASTILLO ORTIZ-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
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
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

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

ADA LUZ SANDOVAL HERAZO-OFICINA CENTRO COMANDO, CONTROL, COMUNICACIONES Y COMPUTO C-4
EDITH NATHALIE ROMERO BARRERA-OFICINA CENTRO COMANDO, CONTROL, COMUNICACIONES Y COMPUTO C-4
ANA CATHERINE MARINO RINCON-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
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
RICHARD OSVALDO GONZALEZ VERA-DIRECCION DE BIENES PARA LA SEGURIDAD, CONVIVENCIA Y ACCESO A LA JUSTICIA
REINALDO RUIZ SOLORZANO-SUBSECRETARIA DE GESTION INSTITUCIONAL
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

Segundo Cuatrimestre - 2025

www.scj.gov.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.

SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA

BOGOTÁ

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 segundo 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 2024, 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 97 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 segundo cuatrimestre se logró la validación y actualización de los activos de información correspondientes al proceso Gestión Documental, proceso Gestión de Recursos Físicos al Servicio de la Entidad, proceso Gestión del Conocimiento y la Innovación Publica y la Oficina del Despacho, los cuales, aunque cuentan con la validación, ajustes y aprobación de los equipos de trabajo de cada proceso, serán publicados en el sitio web institucional al cierre de la vigencia, junto con la actualización integral de los activos de información de toda la Entidad para la vigencia 2025. dentro de esta actualización se validaron 2 activos de información clasificados con criticidad alta para el Proceso Gestión Documental que serán llevados a gestión de riesgos y controles de seguridad de la información de acuerdo a lo establecido en la Política de Administración de Riesgos de la Entidad.

A partir de los 73 activos clasificados con criticidad alta, y conforme a los activos de información del proceso Gestión Documental aprobado previamente mediante acta de reunión, se identificaron y estructuraron 35 riesgos asociados a la seguridad de la información, para los cuales se definieron un total de 47 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. 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 agosto 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 “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/Gobierno TI/MIPG/Riesgos/Seguridad%20Informaci%C3%B3n/Informes/2025/Segundo%20Cuatrimestre/Piezas%20Graficas?csf=1&web=1&e=kdppUP

Gráfica.1 Elaboración Uso y Apropiación DTSI.

Adicionalmente, la Dirección de Tecnologías y Sistemas de la Información (DTSI) emitió el memorando electrónico digital 3-2025-31544 del 08 de agosto 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 mayo, junio, julio y agosto (segundo 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/Informes/2025/Segundo%20Cuatrimestre/Memorando%20Cargue%20Evidencias?csf=1&web=1&e=piGoec

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 segundo 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 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/Gobierno TI/MIPG/Riesgos/Seguridad%20Informaci%C3%B3n/Informes/2025/Segundo%20Cuatrimestre/Comunicaciones%20Electronicas?csf=1&web=1&e=BW9bgM

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

En el transcurso del segundo cuatrimestre de 2025, personal de la Dirección de Recursos Físicos y Gestión Documental y la Dirección de Tecnologías y Sistemas de la Información (DTSI), realizaron las actividades establecidas para la actualización de activos de información de acuerdo al cronograma para todas las áreas y procesos de la Entidad.

Dentro de las actividades más relevantes se logró la actualización de los activos de información para los procesos Gestión Documental, proceso Gestión de Recursos Físicos al Servicio de la Entidad, proceso Gestión del Conocimiento y la Innovación Publica y la Oficina del Despacho, de acuerdo a las actividades establecidas en el plan de actualización de activos de información de la Entidad para la presente vigencia.

Cabe resaltar que la matriz F-GD-1081 - registro de activos de información e índice de información clasificada y reservada de información será publicada en el sitio web de la Entidad al cierre de la vigencia, junto con la actualización integral de los activos de información de los procesos de la Entidad correspondiente a la vigencia 2025.

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/Gobierno TI/MIPG/Riesgos/Seguridad%20Informaci%C3%B3n/Informes/2025/Segundo%20Cuatrimestre/Activos%20de%20Informaci%C3%B3n?csf=1&web=1&e=Cw6qlw

3. Identificación del riesgo.

Para el segundo 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:

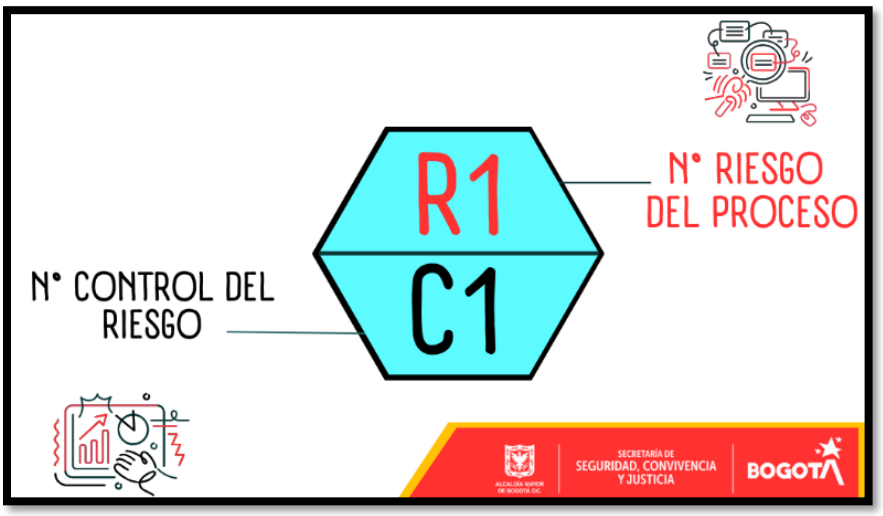
- **WEB**: https://scj.gov.co/es Transparencia y Acceso a la información pública - Planeación, políticas lineamientos y manuales -Plan de acción - Matriz de riesgos Seguridad de la Información – 2025.
  https://scj.gov.co/es/transparencia/planeacion-presupuesto-ingresos/plan-accion

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 de la Entidad.

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



Grafica 2. Nomenclatura Riesgos.

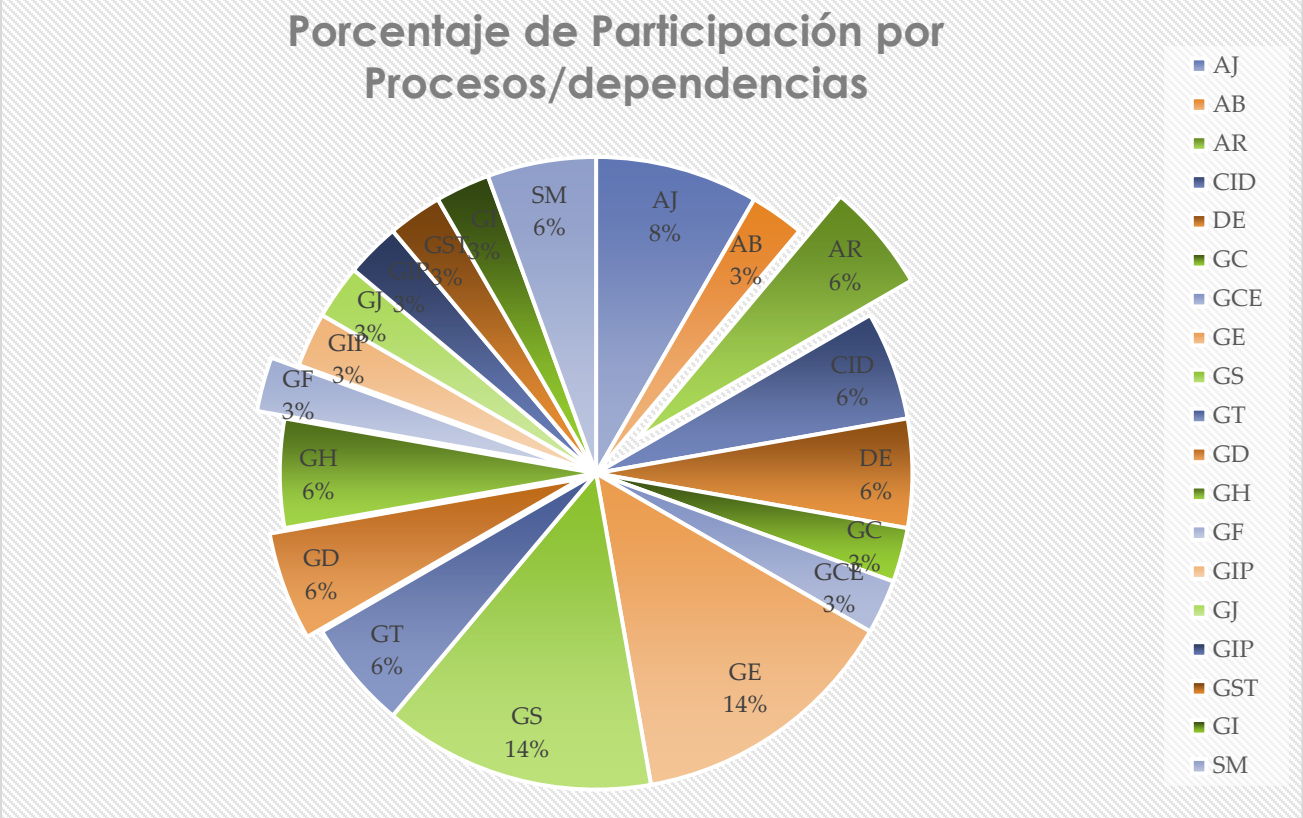
Los Riesgos de seguridad de la información se agrupan por Procesos/dependencia de la siguiente forma:

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**	**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	**35**

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%

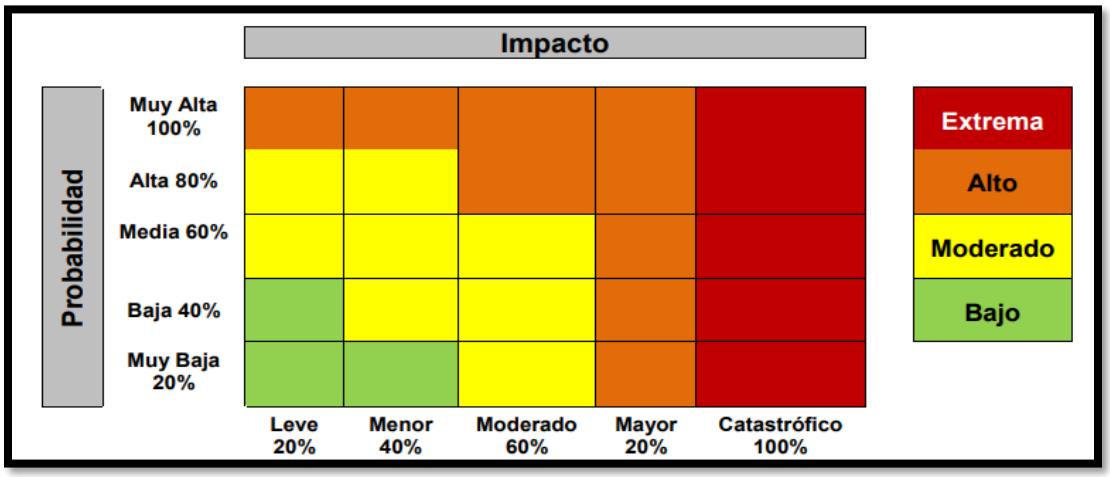
Grafica 4. Fuente: Política de Administración de Riesgos SDSCJ.

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)			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**	**29**	**2**	**35**

Tabla 3. Valoración Riesgos SDSCJ

Dado que es fundamental asegurar la continuidad y correcta ejecución de los procedimientos establecidos en los procesos, no se eligió la opción de “Evitar” como forma de tratar los riesgos identificados. En su lugar, los procesos decidieron aplicar la medida de “Reducir el riesgo”, lo que implica implementar controles que ayuden a disminuir la probabilidad de que dichos riesgos ocurran, de acuerdo 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 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)	**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**	**1**
Total	**35**	**47**

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 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	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.
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 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.
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	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.
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 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.
R11-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.
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 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.
R13-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.
R14-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.

R15-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.
R15-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.
R15-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.
R16-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.
R17-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.
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 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.
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 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.
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 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.
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 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
R26-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.
R26-C2	Gestión de Tecnología de Información	Pérdida de Confidencialidad, integridad y/o	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

		disponibilidad de la información	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.
R27-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.
R27-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.
R27-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
R28-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.
R29-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.
R30-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.
R31-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.
R32-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.
R33-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.
R34-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.
R34-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.
R35-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.

Para el segundo cuatrimestre se agregaron dos (02) riesgos y (04) cuatro controles pertenecientes al proceso Gestión Documental de acuerdo a la actualización de activos de información del área.

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.

La Dirección de Tecnologías y Sistemas de la Información (DTSI) brindó un acompañamiento constante a todos los procesos de la Entidad, con el objetivo de apoyar el cumplimiento de los lineamientos relacionados con la gestión de riesgos de seguridad de la información. Este respaldo se reflejó en orientación técnica, coordinación entre procesos y seguimiento a las actividades necesarias, lo que permitió lograr una implementación efectiva de los controles establecidos.

Gracias a este trabajo conjunto, se logró implementar de manera efectiva las medidas de tratamiento del riesgo, lo cual ha contribuido de forma significativa a reducir las amenazas identificadas y a fortalecer la gestión del riesgo a nivel institucional.

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)			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**	**35**	**2**		**0**	**0**	**0**	**35**

Tabla 6. 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 # 3-2025-24957, correspondiente al "Informe de seguimiento a riesgos de seguridad de la información - primer 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 – Primer Cuatrimestre.

7.1.1. Observación 1: Falta de inclusión del proceso de gestión del conocimiento en el registro de activos de información

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

En atención a la observación relacionada con la falta de inclusión del proceso de Gestión de Conocimiento e Innovación Pública en el registro de activos de información, se informa que se llevaron a cabo mesas de trabajo con los responsables del proceso de la Oficina Asesora de Planeación con el fin de identificar, clasificar y actualizar los activos de información correspondientes.

Dichos activos fueron incorporados en el formato F-GD-1081 - Registro De Activos De Información E Índice De Información Clasificada Y Reservada, garantizando su alineación con las directrices establecidas en la G-FI-04 Guía De Administración De Riesgos, fortaleciendo así la gestión documental y contribuyendo a la identificación y mitigación de riesgos asociados a la seguridad de la información.

Nota aclaratoria: La actualización del registro de activos de información se realiza de manera anual y se publica en el sitio web institucional una vez se consolide la totalidad de los activos de información de la Entidad, asegurando consistencia, integridad y disponibilidad de la información para todos los procesos, de acuerdo con lo establecido en la G-GD-01- Guía De Gestión De Activos De Información E Índice De Información Clasificada Y Reservada.

Documentación Mesas de Trabajo:

Las mesas de trabajo llevadas a cabo por la Dirección de Tecnologías y Sistemas de la Información, en conjunto con la Oficina Asesora de Planeación, para la atención de la observación 1: "*Falta de inclusión del proceso de gestión del conocimiento en el registro*

de activos de información" fueron documentadas mediante la elaboración de su respectiva acta, así:

- Acta proceso de Gestión de Conocimiento e Innovación Pública.
- Formato F-GD-1081- proceso de Gestión de Conocimiento e Innovación Pública.

La documentación está disponible 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/Segundo%20Cuatrimestre/Observaciones/Observaci%C3%B3n%201?csf=1&web=1&e=stoX4T

7.1.2. Observación 2: inconsistencias en la valoración de la probabilidad o impacto con base en las vulnerabilidades.

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

Atendiendo la observación relacionada con las inconsistencias en la valoración de la probabilidad e impacto con base en las vulnerabilidades, se llevaron a cabo mesas de trabajo con las siguientes áreas, con el fin de revisar, validar y ajustar la matriz de riesgos de seguridad de la información, así:

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

En la valoración de los riesgos de seguridad de información del proceso Administración De Bienes Muebles E Inmuebles Para El Fortalecimiento De Las Capacidades Operativas (AB), para el riesgo 4 se ajustan la calificación de probabilidad e impacto para todos los controles establecidos.

Gráfica 7. Ajustes Valoración Riesgos Bienes

- **Proceso Gestión Emergencias (GE)**

En el marco de la identificación del riesgo asociado al proceso de Gestión de Emergencias (GE), y en atención a las observaciones realizadas, se procedió a revisar el riesgo # 15 para dicho proceso. Como resultado de esta revisión, se ajustaron las calificaciones de probabilidad e impacto, asegurando que la valoración de los riesgos se encuentre alineada con las vulnerabilidades identificadas, con los criterios metodológicos

institucionales y con los lineamientos establecidos en la *Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – Versión 6 del DAFP*.

16	Gestión de Emergencias.	NUSE 123 (Número Único de Seguridad y Emergencia Telefonía y CAD (Bitácora Incidente Procedente creado en el sistema CAD), Grabación de Llamada del usuario a Línea de Emergencias 123)	Información	Pérdida de la Confidencialidad	Fallas del equipo.	Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad. Ausencia del personal. Gestión deficiente de las contraseñas.	Demoras en los servicios prestados y ejecución de los procesos	X		Baja	Moderado	MODERADO

Gráfica 8. Ajustes Valoración Riesgos Gestión Emergencias

- **Proceso Gestión de Seguridad y Convivencia. (GS)**

En el marco de la identificación del riesgo asociado al proceso de Gestión de Seguridad y Convivencia. (GS) y en atención a las observaciones realizadas, se procedió a revisar el riesgo # 20 para dicho proceso. Como resultado de esta revisión, se ajustaron las calificaciones de probabilidad e impacto, asegurando que la valoración de los riesgos se encuentre alineada con las vulnerabilidades identificadas, con los criterios metodológicos institucionales y con los lineamientos establecidos en la *Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – Versión 6 del DAFP*

- **Proceso Gestión de Tecnologías de la Información (GT).**

En la identificación del riesgo de del proceso Gestión de Tecnologías de la Información (GT), para los riesgos 25 y riesgo 26 se ajustan la calificación de probabilidad e impacto para todos los controles establecidos, generando un nuevo resultado del riesgo Inherente moderado, validando las consideraciones del riesgo y tomando como referencia los ajustes propuestos por la Oficina de Control Interno.

25	Gestión de Tecnologías de la Información.	Soluciones Tecnológicas SDSCJ (Sistemas de Información, Servicios Ciudadanos Digitales y Servicios Tecnologicos)	Software	Pérdida de CConfidencialidad, integridad y/o disponibilidad de la información	Ciberataque Modificación de bases de datos	Obsolecencia y brechas de seguridad por uso de versionamiento desactualizado del entorno de desarrollo de los diferentes sistemas de información. Falta de Arquitectura de datos estandarizada para los sistemas de información
26	Gestión de Tecnologías de la Información.	Infraestructura Y Plataforma Tecnológica SDSCJ	Hardware	Pérdida de Confidencialidad, integridad y/o disponibilidad de la información	"Uso no autorizado de credenciales de administración a cualquiera de los componentes de la infraestructura de la SDSCJ Ciberataque o incidente informático a la infraestructura del proveedor de nube Ciberataque dirigido a la infraestructura de la Entidad"	No se cuenta con un mecanismo seguro y estandarizado de manejo de credenciales de administración a la infraestructura tecnologica Configuración incorrecta de parámetros.

Gráfica 9. Ajustes Valoración Riesgos Tecnologías de la Información

- **Proceso Gestión Tecnológica de Seguridad y Emergencias (GST).**

En el marco de la identificación del riesgo asociado al proceso Gestión Tecnológica de Seguridad y Emergencias (GST) y en atención a las observaciones realizadas, se procedió a revisar el riesgo # 34 para dicho proceso. Como resultado de esta revisión, se ajustaron las calificaciones de probabilidad e impacto, asegurando que la valoración de los riesgos se encuentre alineada con las vulnerabilidades identificadas, con los criterios metodológicos institucionales y con los lineamientos establecidos en la *Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – Versión 6 del DAFP*.

34	Gestión Tecnológica de Seguridad y Emergencias.	Sistema de Videovigilancia Ciudadana	Hardware	Pérdida de Confidencialidad, Integridad y/o disponibilidad de la información	Falla en equipo de telecomunicaciones.	Trabajo no supervisado del personal externo o de limpieza. Ausencia de acuerdos de nivel de servicio o insuficiencia en los mismos.	Deficiencias o deterioro del servicio al ciudadano	X		Baja	Moderado	MODERADO

Gráfica 10. Ajustes Valoración Riesgos Tecnologías de la Información

En el marco de dichas sesiones se realizó la reevaluación de los criterios aplicados para la estimación de probabilidad e impacto, asegurando su coherencia con las vulnerabilidades identificadas y en cumplimiento de lo establecido en la *Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – Versión 6 del DAFP*.

Como resultado, se fortaleció la consistencia metodológica de la matriz de riesgos, garantizando una mayor trazabilidad en la valoración y una alineación efectiva con los lineamientos institucionales de gestión del riesgo y seguridad de la información.

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 2: "*inconsistencias en la valoración de la probabilidad o impacto con base en las vulnerabilidades*" fueron documentadas mediante la elaboración de sus respectivas actas, así:

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

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/Segundo%20Cuatrimestre/Observaciones/Observaci%C3%B3n%202?csf=1&web=1&e=L1FKC1

7.1.3. 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.

7.1.3.1 Proceso Acceso y Fortalecimiento a la Justicia.

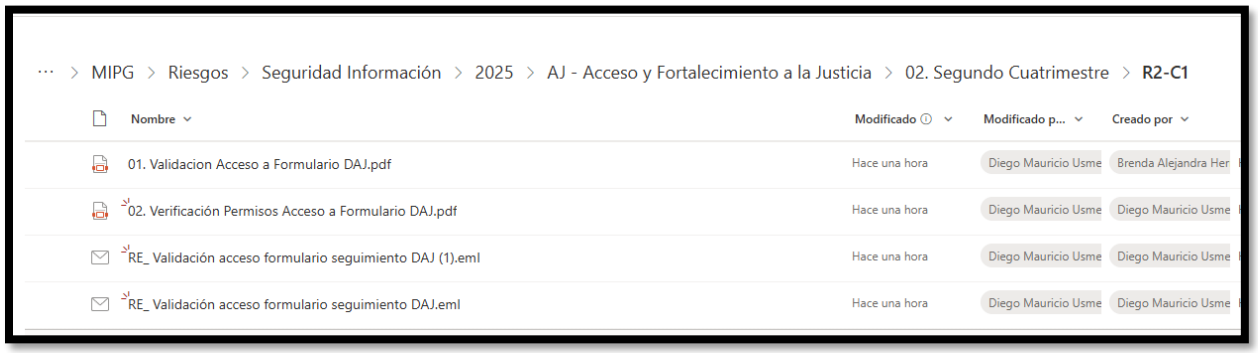
Recomendación riesgo 2 – control 1: Revisión y ajustes de evidencias

El proceso aportó el correo electrónico del día 23/04/2025, mediante el cual se solicita confirmar si se tiene acceso a la carpeta "Informes de Gestión 2025". Sin embargo, no se aportó evidencia que respalde la verificación de permisos derecho de acceso a formularios conforme a lo establecido en el control, así como, no se aporta soporte documental de la acción ante la desviación, el cual indica que: “En caso de que los usuarios no tengan autorización, se retirarán los permisos de acceso y se informará de las acciones al Jefe de área”.

Recomendación: Aportar evidencia de la verificación de permisos y de las acciones tomadas en caso de accesos no autorizados, de conformidad con los lineamientos del control establecido.

Atención a recomendación:

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 segundo cuatrimestre de riesgos de seguridad de Información se presentara de acuerdo con las recomendaciones de la OCI.



Gráfica 11. Cargue Evidencias Riesgo 2 – Control 1

7.1.3.2 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.

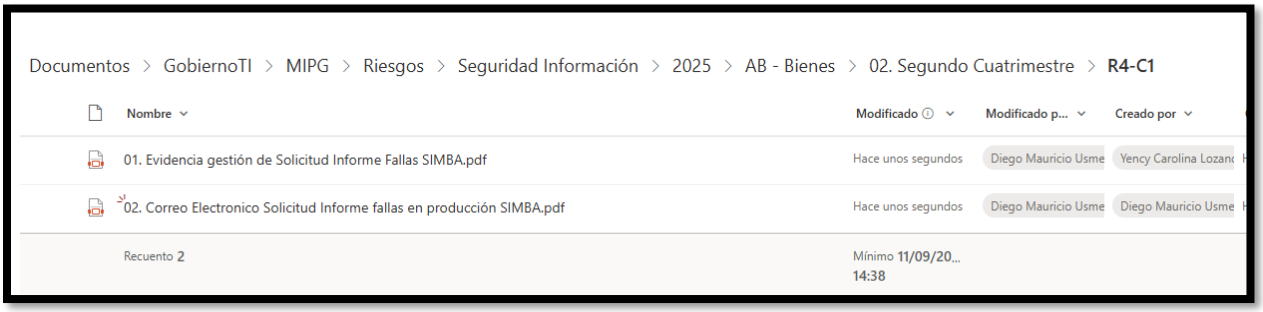
No se aportó evidencia que respalde la ejecución de la actividad de control como el reporte mensual de fallas de producción, el cual se solicita mediante correo electrónico o comunicado oficial a la DTSI, adicionalmente, no se aportó evidencia de la acción ante la desviación "en caso de no entregar el reporte se debe informar al director de Bienes con las acciones para dar cumplimiento".

Recomendación: Establecer mecanismos que aseguren la trazabilidad y documentación de la ejecución de las actividades de control, tales como el reporte mensual de fallas de

producción. Adicionalmente, se sugiere documentar las acciones tomadas en caso de incumplimientos, de conformidad con lo establecido en el control.

Atención a recomendación:

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



Gráfica 12. Cargue Evidencias Riesgo 4 – Control 1

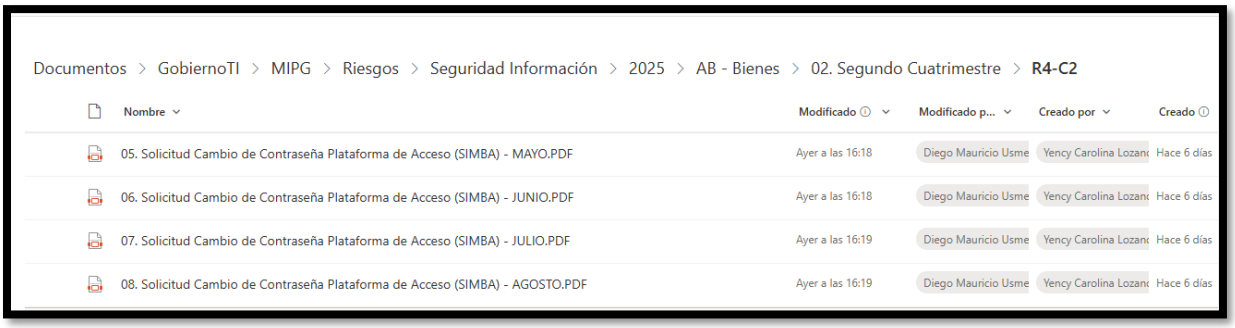
❖ Recomendación Riesgo 4 – Control 2: Revisión y ajustes de evidencias.

La evidencia aportada no permite verificar la ejecución de la actividad de control, debido a que no se aportó evidencia que dé cuenta de las solicitudes mensuales comunicando los talleres, tan solo se evidencian correos en donde se solicita cambios de contraseñas uno del mes de diciembre 2024 que no aplicaría y otro en el mes febrero 2025; adicionalmente, no se aportó evidencia de la acción ante la desviación "En caso de no realizar la solicitud dentro de la vigencia del mes se informará al director de bienes los motivos y las acciones para enviar la notificación, como evidencia se entregara la solicitudes de cambio de contraseña a los talleres".

Se requiere establecer un registro formal y verificable de las solicitudes mensuales a los talleres, así como documentar las acciones tomadas ante incumplimientos, conforme a lo definido en el control.

Atención a recomendación:

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 segundo cuatrimestre de riesgos de seguridad de Información 2025 se presentaran las evidencias del cargue del control de acuerdo con las recomendaciones de la OCI.



Gráfica 13. Cargue Evidencias Riesgo 4 – Control 1

❖ Recomendación Riesgo 4 – Control 3: Revisión y ajustes de evidencias.

La evidencia aportada no permite verificar la ejecución de la actividad de control, debido a que se observa un acta de asistencia correspondiente al mes de octubre de 2024, la cual no aplica para el periodo evaluado, y otra del 31 de enero de 2025 relacionada con la capacitación sobre SIMBA dirigida a supervisores y apoyos técnicos del Grupo Movilidad; sin embargo, no se evidencia la participación de los demás funcionarios y contratistas, adicional la periodicidad es cuatrimestral y no hay registros.

Recomendación: Se hace necesario asegurar el cumplimiento de la actividad de control mediante la programación y documentación oportuna de las capacitaciones conforme a la periodicidad establecida. Asimismo, se debe garantizar la participación de todos los funcionarios y contratistas, dejando evidencia formal y completa de asistencia para el periodo evaluado.

Atención a recomendación:

Para esta recomendación, Pese que el título del acta se establece para capacitación sobre SIMBA dirigida a supervisores y apoyos técnicos del Grupo Movilidad, esta capacitación se realizó de forma general para funcionarios y contratistas tal como se evidencia en el listado de asistencia adjunto al acta.

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 segundo cuatrimestre de riesgos de seguridad de Información 2025 se presentaran las evidencias del cargue del control de acuerdo con las recomendaciones de la OCI.

Gráfica 14. Cargue Evidencias Riesgo 4 – Control 3

7.1.3.3 Proceso de Gestión de Emergencias (GE).

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

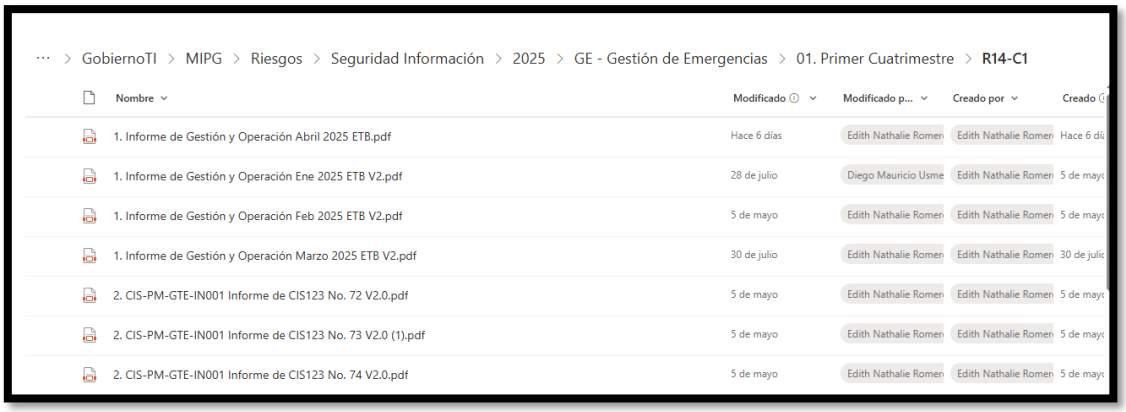
La evidencia aportada no permite verificar la ejecución completa de la actividad de control, ya que el proceso presentó los informes de gestión y operación correspondientes a los meses de enero y febrero de 2025, así como el de diciembre de 2024, este último no aplicable al periodo evaluado. También se aportaron tres informes de apoyo y dos de supervisión; sin embargo, se encuentran pendientes los correspondientes a los meses de marzo y abril de 2025. Adicionalmente, no se evidencian las gestiones realizadas ante la ausencia de reportes por parte del operador tecnológico, tal como lo indica el control: 'En caso de no contar con los reportes que entrega el operador tecnológico, se realizarán las gestiones pertinentes mediante comunicado oficial y/o correo electrónico sobre la solicitud de información".

Recomendación: Fortalecer el seguimiento a la ejecución de la actividad de control mediante la presentación completa y oportuna de los informes de operación, apoyo y supervisión correspondientes a cada periodo. Asimismo, se sugiere

<u>Atención a recomendación:</u>

Para esta recomendación, se informa por parte del equipo de trabajo del proceso de Gestión de Emergencias (GE), se realizó el cargue de información de acuerdo con las recomendaciones generadas por la OCI, en lo que corresponde a los documentos pendientes los correspondientes a los meses de marzo y abril de 2025:

- Informes de gestión y operación correspondientes a los meses de marzo y abril de 2025.
- Informes de apoyo de marzo y abril.
- Informe supervisión OPS mes de febrero, marzo y abril.



Grafica 15. Cargue Evidencias R14–C1

Dentro de las evidencias presentadas se establece que en el próximo cumplimiento para el segundo 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 el correo electrónico del cargue de la información de SOARS correspondiente al primer cuatrimestre del año en el SharePoint, No obstante, al no aportar el link de acceso no se puede validar la existencia de la copia de seguridad de la base de datos incidentes SOARS en el repositorio establecido.

Recomendación: Se sugiere que, al momento de cargar información en el repositorio de SharePoint, se incluya de forma explícita el enlace de acceso al archivo o carpeta correspondiente. Esto permitirá validar la existencia de la copia de seguridad de la base de datos de incidentes SOARS y garantizará la trazabilidad y disponibilidad de la información cargada para su revisión y auditoría.

<u>Atención a recomendación:</u>

En la validación de las observaciones realizadas por la Oficina de Control Interno respecto al enlace de acceso, el equipo estructurador de riesgos de seguridad de la información del C-4 indicó que no es posible entregarlo, dado que los reportes contienen información reservada y clasificada. No obstante, se acordó que en el próximo reporte del segundo cuatrimestre de riesgos de seguridad de la información se fortalecerá la entrega de evidencias y se presentarán conforme a las recomendaciones de la OCI.

Grafica 16. Cargue Evidencias R17–C1

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

Aunque el proceso reporta el correo electrónico del cargue de la información de SOARS correspondiente al primer cuatrimestre del año en el SharePoint. No aportó la evidencia que permita validar la realización del cargue de la copia mensual de seguridad de la bitácora de transferencia de mando del área de seguimiento en el repositorio establecidos en el C-4

Recomendación: Adjuntar evidencia verificable del cargue mensual de la copia de seguridad de la bitácora de transferencia de mando del área de seguimiento en el repositorio C-4, ya que el correo reportado no permite validar dicha acción.

Atención a recomendación:

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

Grafica 17. Cargue Evidencias R18–C1

7.1.3.4 Proceso Gestión de Seguridad y Convivencia (GS).

- Recomendación riesgo 24 – control 1: Revisión y ajustes de evidencias.

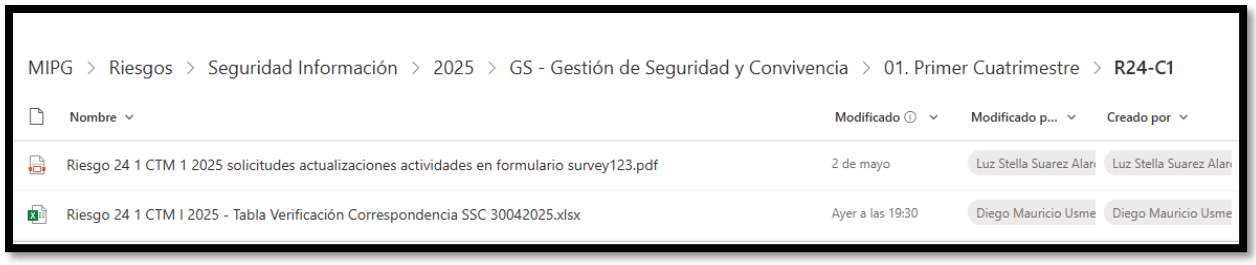
La evidencia aportada no permite verificar la ejecución de la actividad, ya que el proceso únicamente presentó un correo de solicitud para adelantar las acciones necesarias orientadas al registro de la información pendiente en el formulario SURVEY 123. Por otra parte, se encuentra pendiente la entrega de la Tabla de Verificación de Correspondencia, la cual es fundamental para confirmar el avance y cumplimiento de la actividad correspondiente.

Recomendación: Se sugiere complementar la evidencia con documentación que respalde la ejecución efectiva de la actividad, incluyendo la Tabla de Verificación de Correspondencia debidamente actualizada y validada por los responsables del proceso.

Atención a recomendación:

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

• Tabla de Verificación de Correspondencia.



Grafica 18. Cargue Evidencias R24–C1

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

7.1.3.5 Proceso Gestión de Tecnología de Información (GT)

- ❖ Recomendación riesgo 26 - control 1: Ajustar Evidencias.

La evidencia aportada no permite verificar la ejecución de la actividad de control en su totalidad, debido a que si bien el proceso aportó un documento titulado Mecanismo de gestión segura de contraseñas, que tiene como objetivo “Establecer y mantener un sistema robusto y eficiente para la gestión de credenciales de administración que garantice la seguridad, integridad y accesibilidad de los sistemas de información de la SDSCJ, no se aportó evidencia que dé cuenta del seguimiento trimestral al cumplimiento de los mecanismos establecidos, asimismo, no se tienen registros de la acción ante la desviación en caso de no contar con el seguimiento.

Recomendación: se hace necesario ajustar lo que indica el soporte de la actividad de control, toda vez, que es necesario incluir el reporte con el seguimiento trimestral.

Atención a recomendación:

Para este control, el Grupo de Sistemas de Información establecerá los ajustes y actualizaciones necesarias que permitan fortalecer la gestión del riesgo, garantizar la eficacia del control y asegurar la alineación con los lineamientos institucionales en materia de seguridad de la información.

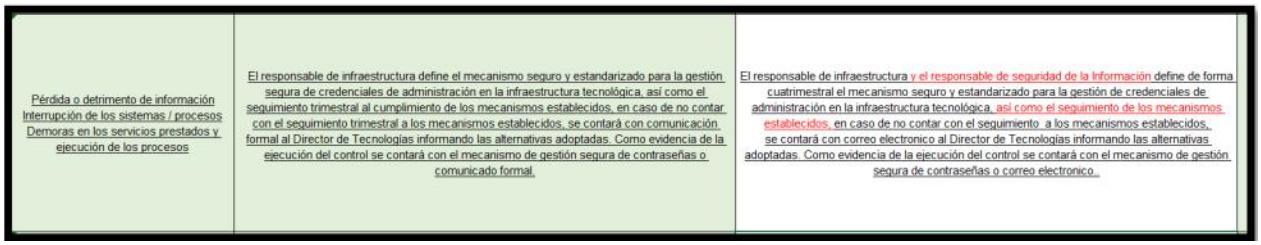
Control Actual:

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.

Proyección y ajustes del control:

Se realizan ajustes al control conforme a las consideraciones definidas por el grupo de trabajo de la Dirección de Tecnologías y Sistemas de Información (DTSI):

"*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."*



Pérdida o detrimento de información Interrupción de los sistemas / procesos Demoras en los servicios prestados y ejecución de los procesos	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.	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 electronico 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 electronico.

Grafica 19. Ajuste Control R26–C1

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 segundo cuatrimestre de riesgos de seguridad de Información se presentarán las evidencias del cargue del control de acuerdo con las recomendaciones de la OCI.

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

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

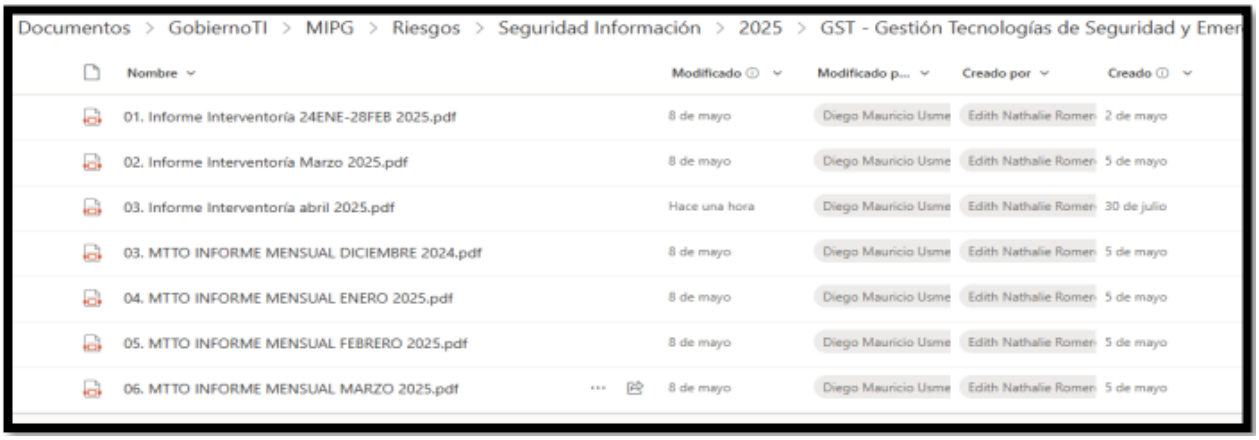
Se evidencia la ejecución parcial de la actividad, mediante la presentación de los informes mensuales de interventoría correspondientes a los meses de enero, febrero y marzo de 2025. Sin embargo, se encuentra pendiente la entrega del informe correspondiente al mes de abril, así como los reportes de seguimiento a los mantenimientos realizados durante el mismo período.

Recomendación: Se recomienda consolidar y presentar la información pendiente para completar la trazabilidad del control establecido, asegurando la continuidad en el seguimiento y la documentación de las actividades ejecutadas.

Atención a recomendación:

Para esta recomendación, se informa por parte del equipo de trabajo del proceso de Gestión Tecnológica de Seguridad y Emergencias (GST), se realiza el cargue de información de acuerdo con las recomendaciones generadas por la OCI, así:

• Reportes de Interventoría mes Abril.
• Reporte Mensual Mantenimiento mes Abril.



Grafica 20. Cargue de Evidencias R32–C1

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

- ❖ Recomendación riesgo 32 - 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.
Recomendación: Se sugiere realizar el seguimiento respectivo para garantizar la entrega oportuna del informe de abril, a fin de mantener la continuidad y trazabilidad del control establecido.

Atención a recomendación:

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

• Reporte Mensual Mantenimiento mes Abril.

Grafica 21. Cargue de Evidencias R32–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 segundo cuatrimestre de riesgos de seguridad de Información se entregara de acuerdo con las recomendaciones de la OCI.

7.1.4. Gestión y Análisis de Información (GI).

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

La evidencia aportada no permite validar la ejecución de la actividad de control, ya que únicamente se presentaron los archivos en Excel correspondientes a la "Consulta Actualización Bodega" del primer cuatrimestre de 2025. Sin embargo, no se anexó la evidencia del indicador de gestión asociado, lo cual impide confirmar el cumplimiento efectivo de la actividad.

Recomendación: Se sugiere complementar la información suministrada con el reporte o soporte del indicador de gestión correspondiente, debidamente actualizado y validado, que permita verificar el impacto y cumplimiento de la actividad de control ejecutada.

Atención a recomendación:

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

Grafica 22. Ajuste Cargue Evidencias R33–C1

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).
- Gestión de Seguridad y Convivencia (GS).
- Gestión de Tecnología de Información (GT).
- Gestión y Análisis de Información (GI)

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/Segundo%20Cuatrimestre/Observaciones/Observaci%C3%B3n%203?csf=1&web=1&e=ksh5Qd

7.2 Oportunidades de Mejora - Oficina Control Interno – Primer 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 sobre la falta de publicación de una versión actualizada de la matriz de activos de información correspondiente al primer cuatrimestre de 2025, se informa que, en el marco del Plan de Actualización de Activos de Información, por parte de la Dirección de Recursos Físicos y Gestión Documental y la Dirección de Tecnologías y Sistemas de la Información, se han venido adelantando mesas de trabajo con todos los procesos y áreas de la Entidad, orientadas a la actualización de los activos de información para la vigencia 2025.

Es importante precisar que, de acuerdo con la metodología institucional, la actualización del registro de activos de información se realiza de forma anual, consolidando los resultados al cierre de la vigencia. Una vez completado este proceso, la versión oficial consolidada es publicada en el sitio web institucional y en datos abiertos Bogotá, garantizando así consistencia, trazabilidad y alineación con los lineamientos de gestión documental y de seguridad de la información.

Como soporte, se aportan las evidencias parciales de las mesas de trabajo y actividades realizadas durante el periodo de referencia, las cuales reflejan los avances obtenidos en los diferentes procesos y áreas, en espera de su consolidación final para la publicación oficial correspondiente.

Documentación Mesas de Trabajo:

Las mesas de trabajo y actividades llevadas a cabo por la Dirección de Recursos Físicos y Gestión Documental y la Dirección de Tecnologías y Sistemas de la Información, en conjunto con las áreas pertinentes, para la atención de la oportunidad de Mejora # 1 se evidencias 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/Segundo%20Cuatrimestre/Oportunidades%20Mejora/01.%20Op_Me_1?csf=1&web=1&e=QQ5vXX

7.2.2. Oportunidad de Mejora 2

Oportunidad de Mejora 1 (Primer Cuatrimestre). Falta de inclusión de riesgos y controles de seguridad de la información asociados al proceso de Gestión Documental, después de presentarse un incidente con documentos físicos en la casa de Justicia de San Cristóbal en la vigencia 2024.

Recomendación: Priorizar la identificación, análisis y documentación de los riesgos antes del segundo trimestre de 2025. Esto permitirá anticipar posibles inconvenientes, optimizar la toma de decisiones y garantizar una planificación eficiente. Además, se sugiere establecer mecanismos de seguimiento para asegurar el cumplimiento oportuno de esta actividad.

En atención a la observación sobre la falta de inclusión de riesgos y controles de seguridad de la información asociados al proceso de Gestión Documental, se informa que se llevaron a cabo mesas de trabajo de actualización de activos de información, en las cuales se adelantó la identificación, análisis y documentación de riesgos y controles correspondientes a los activos de información calificados con criticidad alta, de acuerdo con los lineamientos definidos en la Política de Administración de Riesgos de la Entidad.

Los riesgos y controles identificados son incorporados en la Matriz de Riesgos de Seguridad de la Información, la cual es publicada en el sitio web institucional una vez consolidada, garantizando visibilidad, trazabilidad y transparencia en la gestión.

Documentación Mesas de Trabajo:

Las mesas de trabajo y actividades llevadas a cabo por la Dirección de Recursos Físicos y Gestión Documental y la Dirección de Tecnologías y Sistemas de la Información, sobre la actualización de activos de información y la creación de controles y riesgos de seguridad de la Información, para la atención de la oportunidad de Mejora 1 (Primer Cuatrimestre), así:

- Acta Actualización Activos de Información Proceso Gestión Documental.
- Acta Riesgos de seguridad Información Proceso Gestión Documental.
- Matriz de Riesgos de seguridad Información Proceso Gestión Documental.

Las Actas y Matriz fueron cargadas 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/Informes/2025/Segundo%20Cuatrimestre/Oportunidades%20Mejora/02.%20Op_Me_2?csf=1&web=1&e=8Jz0Jk

7.2.3. Oportunidad de Mejora 3

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

Validar riesgo 4 Bienes control 1 "En este caso específico, la instrucción de "se deberá informar al Director", no incluye detalles sobre las acciones posteriores para su tratamiento que permitan garantizar el cumplimiento de la actividad generada que corrija la desviación detectada.

Control Actual:

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.

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

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.

Interrupción de los sistemas / procesos	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.	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 electronico y/o comunicado oficial por la Dirección de Bienes solicitando el reporte y/o los motivos de la no entrega de esta información.

Grafica 23. Ajuste Control R4–C1

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/Segundo%20Cuatrimestre/Oportunidades%20Mejora/03.%20Op_Me_3?csf=1&web=1&e=5NA85H

7.2.4. Oportunidad de Mejora 4

Oportunidad de Mejora N°4 (Primer Cuatrimestre): Falta de inclusión de tipologías de controles automáticos y manuales en la estructuración de estos dentro de la matriz de riesgos de seguridad de la información.

Recomendación: Se recomienda establecer un plan de trabajo con responsables y tiempos definidos para implementar las acciones previstas a ejecutar “Revisar los controles existentes en la matriz FFI-1385 y clasificarlos según su tipología (automáticos o manuales), Ajustar o incorporar nuevos controles conforme a los riesgos identificados”. Además, es fundamental realizar un seguimiento periódico para verificar el cumplimiento de las medidas adoptadas y garantizar la mejora continua en los procesos.

En atención a la oportunidad de mejora sobre la falta de inclusión de tipologías de controles automáticos y manuales en la estructuración de la Matriz de Riesgos de Seguridad de la Información, se informa que se adelantaron acciones orientadas a fortalecer las recomendaciones establecidas por la Oficina Control Interno así:

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

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

Se realizó la revisión y validación de los controles establecidos en la matriz de riesgos de seguridad de la información, con el fin ajustar y garantizar su adecuada correspondencia frente a los riesgos identificados. así:

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

Adicionalmente, se incorporaron 2 riesgos y 4 controles adicionales, reforzando la cobertura y efectividad de la matriz de riesgos de seguridad de la Información, así:

- Gestión Documental (GD).

De igual manera, se efectuó seguimiento al cargue de evidencias de controles de seguridad de la información, asegurando la validación de su implementación y el cumplimiento de los lineamientos establecidos para la mejora continua.

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/Segundo%20Cuatrimestre/Oportunidades%20Mejora/04.%20Op_Me_4?csf=1&web=1&e=W9KOOq

8. CARGUE EVIDENCIAS

A través del memorando interno No. 3-2025-31544 del 08 de agosto de 2025, emitido por la Dirección de Tecnologías y Sistemas de la Información (DTSI), se solicitó el cargue de información correspondiente al segundo 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 primer cuatrimestre de 2025, 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
AJ	Acceso y Fortalecimiento a la Justicia	**3**	**3**	**10**
AB	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	**1**	**4**	**17**
AR	Atención y Relación con el Ciudadano	**2**	**2**	**8**
CID	Control Disciplinario	**2**	**2**	**2**
DE	Direccionamiento Estratégico.	**2**	**2**	**11**
SM	Evaluación al Sistema de Control Interno	**2**	**3**	**6**
GC	Gestión Contractual	**1**	**1**	**2**
GCE	Gestión de Comunicaciones Estratégicas.	**1**	**1**	**2**
GE	Gestión de Emergencias	**5**	**7**	**23**
GS	Gestión de Seguridad y Convivencia	**5**	**6**	**11**
GT	Gestión de Tecnología de Información	**2**	**4**	**42**
GD	Gestión Documental	**2**	**4**	**11**
GH	Gestión Estratégica del Talento Humano	**2**	**2**	**8**

GF	Gestión Financiera.	**1**	**1**	**2**
GIP	Gestión Integral a las Personas Privadas de la Libertad - PPL.	**1**	**1**	**1**
GJ	Gestión Jurídica	**1**	**1**	**2**
GST	Gestión Tecnológica de Seguridad y Emergencias.	**1**	**2**	**8**
GI	Gestión y Análisis de Información	**1**	**1**	**5**
	Total	**35**	**47**	**171**

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.

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 por parte de los procesos:

# Riesgo	Proceso	Control	Recomendaciones
R15-C1	Gestión de Emergencias	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.	En relación con el seguimiento a la operación, el informe de interventoría y el informe de supervisión del mes de agosto, se establece por parte del equipo estructurador de riesgos para C-4 que estos no se han presentado debido a que actualmente el contratista se encuentra en proceso de elaboración y entrega de estos. Posteriormente, los informes pasan por las fases de validación, ajustes y aprobación por parte del C4, requisito previo para proceder con el trámite de aprobación final y el correspondiente pago. Una vez cumplidas estas actividades de validación y verificación y obtenida la aprobación, el informe será cargado en los repositorios establecidos.
R16-C1	Gestión de Emergencias	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.	El control tiene periodicidad trimestral, por lo cual se cargaron las evidencias correspondientes al segundo trimestre de la vigencia 2025. Las evidencias del tercer trimestre serán cargadas en el próximo proceso de cargue establecido, garantizando su incorporación en los repositorios establecidos para efectos de control y trazabilidad.
R17-C1	Gestión de Emergencias	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	En relación con el seguimiento a los informes de gestión del mes de agosto, se establece se establece por parte del equipo estructurador de riesgos para C-4 que este no se ha presentado debido a que actualmente el contratista se encuentra en proceso de elaboración y entrega

		económicamente. las Evidencia corresponde al Informe mensual de la empresa contratista. El cargue de las evidencias se hará trimestralmente.	de este. Posteriormente, el informe pasa por las fases de validación, ajustes y aprobación por parte del C4, requisito previo para proceder con el trámite de aprobación final. Una vez cumplidas estas actividades de validación y verificación y obtenida la aprobación, el informe será cargado en los repositorios establecidos.
R18-C1	Gestión de Emergencias	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.	El equipo estructurador de C-4 y tomando como referencias las observaciones de la Oficina Control Interno. Establece que, por razones de confidencialidad de la información asociada a los casos registrados en el SOARS, no se compartirán enlaces directos a la información. Cabe resaltar que la Jefatura C-4 cuenta con acceso autorizado a dicha información, garantizando la disponibilidad para su consulta.
R34-C1	Gestión Tecnológica de Seguridad y Emergencias.	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.	En relación con el reporte mensual de los mantenimientos del mes de agosto, se establece se establece por parte del equipo estructurador de riesgos para C-4 que este no se ha presentado debido a que actualmente el contratista se encuentra en proceso de elaboración y entrega de este. Posteriormente, el informe pasa por las fases de validación, ajustes y aprobación por parte del C4, requisito previo para proceder con el trámite de aprobación final. Una vez cumplidas estas actividades de validación y verificación y obtenida la aprobación, el informe será cargado en los repositorios establecidos.
R34-C2	Gestión Tecnológica de Seguridad y Emergencias.	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.	En relación con el reporte mensual la empresa contratista del mes de agosto, se establece se establece por parte del equipo estructurador de riesgos para C-4 que este no se ha presentado debido a que actualmente el contratista se encuentra en proceso de elaboración y entrega de este. Posteriormente, el informe pasa por las fases de validación, ajustes y aprobación por parte del C4, requisito previo para proceder con el trámite de aprobación final. Una vez cumplidas estas actividades de validación y verificación y obtenida la aprobación, el informe será cargado en los repositorios establecidos.

Tabla. 8 – Cargue Evidencias de Controles

9. CONCLUSIONES

En conclusión, al cierre del segundo cuatrimestre del año 2025, la Dirección de Tecnologías y Sistemas de la Información reafirma su compromiso con la gestión integral de la seguridad de la información, garantizando la revisión, actualización y seguimiento permanente de la matriz de riesgos. Esta gestión se ejecuta en concordancia con la Política de Administración de Riesgos y en alineación con los lineamientos de la *Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – Versión 6 (noviembre de 2022)* del DAFP. Dichas actividades han contado con el acompañamiento activo de los líderes operativos de cada área, cuyo rol ha sido fundamental para la correcta implementación y efectividad de los controles establecidos.

Como resultado del seguimiento efectuado durante el segundo cuatrimestre de 2025 a los riesgos de seguridad de la información identificados en los procesos evaluados, se concluye que la gestión realizada ha favorecido la continuidad operativa y el cumplimiento de los objetivos definidos. Este enfoque ha fortalecido la ejecución de actividades críticas y ha contribuido directamente al logro de los objetivos estratégicos de la Entidad en materia de seguridad de la información.

Como resultado 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 3-2025-24957 *“Informe de seguimiento a riesgos de seguridad de la información – primer cuatrimestre de 2025”*, se ha evidenciado un avance relevante en la validación de las observaciones formuladas. Dichas actividades han facilitado una evaluación más precisa de los controles implementados y reflejan el compromiso de las áreas involucradas, cuya participación ha sido determinante para la implementación de las recomendaciones y el fortalecimiento de la efectividad de los controles establecidos.

En concordancia con la Política de Administración de Riesgos de la Entidad, que establece la actualización de los activos de información como un componente esencial para la identificación, valoración, asignación, control y seguimiento de los riesgos de seguridad de la información que puedan impactar el desarrollo de los procesos y el cumplimiento de los objetivos estratégicos, en el segundo cuatrimestre de la vigencia 2025 se han desarrollado actividades establecidas en el plan de actualización de activos de información de acuerdo a programación establecida entre la dirección de Recursos Físicos y Gestión Documental y la Dirección de Tecnologías y Sistemas de la Información. Estas actividades tienen como propósito la actualización del registro de activos de información y del índice de información clasificada y reservada para la vigencia 2025.

Es importante destacar 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 proceso ha contado con la participación de los

líderes operativos de cada área, lo que ha permitido una adopción articulada y coherente de la política durante la presente vigencia, fortaleciendo la gestión institucional en este ámbito.

Se resalta 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 para la gestión de los riesgos de seguridad de la información. En este marco, la Dirección de Tecnologías y Sistemas de la Información extiende un reconocimiento especial a los colaboradores que garantizaron el cumplimiento oportuno de las actividades de seguimiento y el cargue de evidencias durante el segundo cuatrimestre de 2025, contribuyendo de manera significativa 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, ratifica su responsabilidad y disposición para brindar el acompañamiento metodológico requerido en la gestión de riesgos de seguridad de la información durante la vigencia 2025. Este apoyo comprende la orientación frente a eventuales ajustes en las caracterizaciones, procedimientos y documentos que soportan la gestión de cada proceso, lo cual podrá implicar la actualización de riesgos o controles previamente identificados.