ALCALDÍA MAYOR DE BOGOTÁ
SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA
AL RESPONDER CITAR EL NR.
Nro. Rad: 3-2025-1528
Fecha: 16/01/2025 03:09:35 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 TERCER CUATRIMESTRE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN - 2024.

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.: JORGE ELIECER VELASQUEZ PERILLA-DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION
RAFAEL HUMBERTO LOPEZ SAAVEDRA-DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION
ARMANDO ALFONSO LEYTON GONZALEZ-DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION
FRANCISCO ALFORD BOJACA-COBRO PERSUASIVO
OSCAR ALBERTO PORRAS MURCIA-EQUIPO ATENCION AL CIUDADANO
JOHN ALEXANDER HINCAPIE RUEDA-OFICINA ASESORA DE PLANEACION
LAURA JOHANNA GUERRA SALCEDO-OFICINA ASESORA DE PLANEACION
PAOLA ANDREA CHACON TELLEZ-OFICINA ASESORA DE COMUNICACIONES
YESSICA PAOLA NOGUERA BECERRA-OFICINA ASESORA DE COMUNICACIONES
SOONYI ALEJANDRA MUNOZ TORRES-OFICINA DE CONTROL INTERNO
ANDRES ORLANDO TORRES EUSSE-OFICINA DE CONTROL INTERNO
JENNIFER CATHERINE VELASQUEZ-OFICINA DE CONTROL DISCIPLINARIO INTERNO
YAIDE YAMILE ACEVEDO SARMIENTO-OFICINA DE CONTROL DISCIPLINARIO INTERNO
DIANA MARCELA FLECHAS RUIZ-OFICINA DE ANÁLISIS DE INFORMACION Y ESTUDIOS ESTRATEGICOS
JUAN FELIPE CAMPOS CONTRERAS-OFICINA DE ANÁLISIS DE INFORMACION Y ESTUDIOS ESTRATEGICOS
ADA LUZ SANDOVAL HERAZO-OFICINA CENTRO COMANDO, CONTROL, COMUNICACIONES Y COMPUTO C-4
EDITH NATHALIE ROMERO BARRERA-OFICINA CENTRO COMANDO, CONTROL, COMUNICACIONES Y COMPUTO

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

CQR COMPAÑÍA ISO 45001:2018 CERTIFICADA
Certificado No. SG-2022006868

BOGOTÁ

C-4
ANA CATHERINE MARINO RINCON-OFICINA CENTRO COMANDO, CONTROL, COMUNICACIONES Y COMPUTO C-4
SANDRA MILENA PEREZ RAMIREZ-SUBSECRETARIA DE SEGURIDAD Y CONVIVENCIA
ESTEFANIA ESTRADA VILLADA-SUBSECRETARIA DE SEGURIDAD Y CONVIVENCIA
ALBERTO SANCHEZ GALEANO-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
YOLIANA HERNANDEZ ROZO-DIRECCION DE RESPONSABILIDAD PENAL ADOLESCENTE
EFRAIN ARMANDO ZAMBRANO CAMARGO-DIRECCION DE RESPONSABILIDAD PENAL ADOLESCENTE
JOSE LUIS GASCA GONZALEZ-DIRECCION DE BIENES PARA LA SEGURIDAD, CONVIVENCIA Y ACCESO A LA JUSTICIA
ORLANDO VEGA NAVAS-DIRECCION DE BIENES PARA LA SEGURIDAD, CONVIVENCIA Y ACCESO A LA JUSTICIA
REINALDO RUIZ SOLORZANO-SUBSECRETARIA DE GESTION INSTITUCIONAL
JAVIER ALBERTO JIMENEZ VALDERRAMA-DIRECCION DE GESTION HUMANA
DEISY NATALIA VALENCIA GONZALEZ-DIRECCION FINANCIERA
DEIDER MAURICIO MENGUAL PATERNINA-DIRECCION FINANCIERA
VICTOR MANUEL TIQUE-DIRECCION DEL CENTRO ESPECIAL DE RECLUSION
LINA CRISTINA MEDINA SARMIENTO-DIRECCION DEL CENTRO ESPECIAL DE RECLUSION
Anexos: -1

Elaboró: DIEGO MAURICIO USME GONZALEZ
Revisó: DIANA CAMILA MENDEZ RESTREPO-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

CQR COMPAÑÍA ISO 45001:2018 CERTIFICADA
Certificado No. SG-2022006868

BOGOTÁ

INFORME TERCER CUATRIMESTRE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN - 2024

Dirección de Tecnologías y Sistemas de la Información.

Enero de 2025

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA
BOGOTÁ

Contenido

1. INTRODUCCIÓN

En referencia a los parámetros establecidos en la Política de Administración de Riesgos de la Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ (PO-FI-02- Ver. 2), en el ítem 13. Publicación, Seguimiento y Evaluación a los Riesgos, se establece que la Segunda Línea de Defensa para este caso la Dirección de Tecnologías y Sistemas de la Información, "*Corresponde al Profesional de Seguridad de la Información de la Dirección de Tecnologías y Sistemas de la Información. Realiza cuatrimestralmente seguimiento a la Matriz de Riesgos y remitirá informe del resultado a la Oficina de Control Interno, los primeros 10 días hábiles, una vez vencido el cuatrimestre",* El presente informe detalla las actividades realizadas durante el tercer cuatrimestre de la vigencia 2024.

El monitoreo a la matriz de riesgos de seguridad de información se fundamenta en el trabajo previo de actualización de activos de información para la vigencia 2024, donde se validaron un total de 322 activos de información, el personal responsable de cada proceso evaluó estos activos conforme a los principios de Confidencialidad, Integridad y Disponibilidad de información. De esta evaluación, se determinó que 71 activos fueron clasificados con una valoración de criticidad Alta, 154 activos con una valoración de criticidad Media y 97 activos con una valoración de criticidad Baja.

Sobre el ejercicio de levantamiento de riesgos de seguridad de la información se tomaron como referencia los 71 activos de información clasificados con una valoración de criticidad Alta, siendo aprobados en las actividades previas de actualización de activos de información, de lo cual se validaron y estructuraron un total de 33 riesgos y se generaron 43 controles para toda la Entidad.

Lo anterior de acuerdo con los parámetros establecidos en la Política de Administración de Riesgos de la Entidad, así:

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)

DE EVALUCIÓN:

Evaluación al Sistema de Control Interno (SM)
Control Disciplinario (CID)

APOYO:

Gestión Jurídica (GJ)
Gestión Contractual (GC)
Gestión Financiera. (GF)

En líneas generales, cada uno de los procesos y áreas mencionadas ha detectado al menos un riesgo, y todos ellos están en conformidad con los lineamientos establecidos en la Política de Administración de Riesgos PO-FI-02 Ver. 2 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.

2. ACTIVOS DE INFORMACIÓN.

Durante la vigencia 2024, se adelantó por parte de la Dirección de Recursos Físicos y Gestión Documental en acompañamiento con la Dirección de Tecnologías y Sistemas de la Información, mesas de trabajo con todos los procesos y áreas de la Entidad sobre la actualización de activos de información de acuerdo a la actualización de las tablas de retención documental, de lo cual se realizaron mesas de trabajo con cada uno de las áreas de forma presencial y virtual donde se dio amplia información sobre las actividades referentes al diligenciamiento del formato F-GD-1081 “Registro de Activos de Información E Índice de Información Clasificada Y Reservada” para lograr la consolidación de la información requerida, así como el desarrollo de ejercicios prácticos sobre levantamiento y actualización de activos, en la actualización de los activos de información con cada uno de los procesos se consolido la siguiente información, así:

Proceso	Criticidad Alta	Criticidad Media	Criticidad Baja	Total, Activo
Direccionamiento Estratégico	6	3	0	9
Fortalecimiento Institucional	0	1	2	3
Gestión del Conocimiento y la Innovación Pública	0	0	0	0
Gestión de Comunicaciones Estratégicas	1	6	0	7
Evaluación al Sistema de Control Interno	2	9	1	12
Control Disciplinario	5	0	0	5
Gestión y Análisis de la Información	2	1	0	3

Gestión de Emergencias	6	3	0	9
Gestión Tecnológica de Seguridad y Emergencias	1	0	0	1
Gestión de Seguridad y Convivencia	1	6	0	7
Acceso y Fortalecimiento a la Justicia	6	7	0	13
Gestión Integral a las Personas Privadas de la Libertad - PPL	1	41	51	93
Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativa	1	6	1	8
Atención y Relación con el Ciudadano	0	5	7	12
Gestión de Tecnologías de la Información	23	13	32	68
Gestión Estratégica del Talento Humano	8	6	2	16
Gestión Contractual	3	0	0	3
Gestión Jurídica	1	4	0	5
Gestión de Recursos Físicos al Servicio de la Entidad	0	15	0	15
Gestión Documental	0	8	1	9
Gestión Financiera	4	20	0	24
Total	**71**	**154**	**97**	**322**

Tabla 1. Activos de Información.

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

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

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

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

3. SOCIALIZACIÓN RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

En referencia a las actividades de socialización, por parte de la Dirección de Tecnologías y Sistemas de la Información - DTSI, se remitió memorando electrónico digital 3-2024-42215 de fecha 12/12/2024 – DTSI donde se brinda información referente al cargue de evidencias para los controles establecidos para mitigar los riesgos de Seguridad de la información para los meses de septiembre, octubre, noviembre y diciembre (Tercer Cuatrimestre vigencia 2024) para los procesos y áreas definidas, en el siguiente enlace:

https://scjgovcol.sharepoint.com/:b:/r/sites/DireccionTIC/Documentos%20compartidos/GobiernoTI/MIPG/Riesgos/Seguridad%20Informaci%C3%B3n/Informes/2024/Tercer%20Cuatrimestre/Memorando/3-2024-42215_1.pdf?csf=1&web=1&e=KPMrlX

Así mismo, se realizó por parte de la DTSI, difusión a través de correo electrónico a todas y cada una de las áreas que manejan riesgos de seguridad de la información, donde se entrega información referente al cargue de evidencias para el segundo cuatrimestre, así como la validación de las observaciones presentados por parte de la Oficina de Control Interno sobre el

informe de riesgos de seguridad de la Información del segundo cuatrimestre 2024, las evidencias se encuentran en el siguiente enlace:

https://scjgovcol.sharepoint.com/:f:/r/sites/DireccionTIC/Documentos%20compartidos/GobiernoTI/MIPG/Riesgos/Seguridad%20Informaci%C3%B3n/Informes/2024/Tercer%20Cuatrimestre/Comunicaciones%20Electronicas?csf=1&web=1&e=bSlonq

Por otra parte, durante el mes de diciembre 2024 se llevó a cabo el diseño y la presentación de una pieza gráfica titulada “Cargue de Evidencias a Riesgos de Seguridad de la Información”, la cual fue difundida de manera masiva a toda la Entidad. Las evidencias correspondientes se encuentran cargadas en el siguiente enlace:

https://scjgovcol.sharepoint.com/:f:/r/sites/DireccionTIC/Documentos%20compartidos/GobiernoTI/MIPG/Riesgos/Seguridad%20Informaci%C3%B3n/Informes/2024/Tercer%20Cuatrimestre/Pieza%20Grafica?csf=1&web=1&e=MSVPo7

Gráfica.1 Elaboración Uso y Apropiación DTSI.

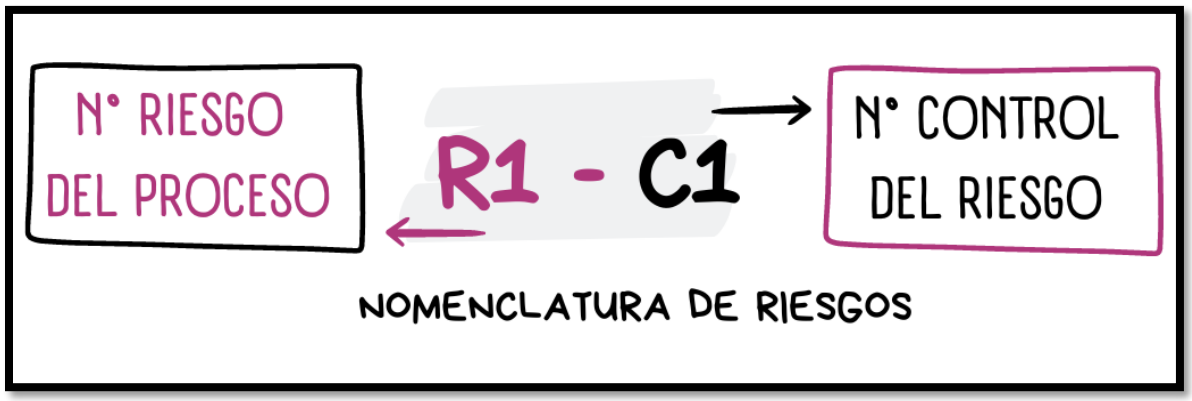
4. MATRIZ DE RIESGOS DE SEGURIDAD DE INFORMACIÓN

Para el tercer cuatrimestre del 2024, se dio gestión a la "Matriz de Riesgos de Seguridad de la información", la cual está disponible en la página WEB de la SDSCJ, en la siguiente ruta:

- **WEB**: https://scj.gov.co/es Transparencia y Acceso a la información pública - Planeación, políticas lineamientos y manuales -Plan de acción - Matriz de riesgos Seguridad de la Información – 2024.
  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 que consolida los riesgos de los procesos, incluyendo la hoja de resumen, el listado de activos, el riesgo inherente, los tratamientos de riesgo, la valoración con controles y el tratamiento del riesgo residual.
- Todos los Riesgos y controles se gestionan de acuerdo con la metodología definida en la Política de Administración de Riesgos.
- La nomenclatura de cada riesgo se define según los siguientes criterios:



Grafica 2. Nomenclatura de Riesgos

4.1. Recomendaciones OCI.

En referencia a las conclusiones y recomendaciones generadas por la Oficina de Control Interno (OCI) mediante el radicado 3-2024-34703 "Informe de Seguimiento a Controles asociados a los Riesgos de Seguridad de la Información correspondiente al segundo cuatrimestre de 2024" de fecha 21/10/2024, Se llevaron a cabo mesas de trabajo con todas las áreas y procesos para recopilar la información relacionada con la atención a las observaciones de la Oficina de Control Interno y el seguimiento a los controles de los riesgos de seguridad de la información correspondientes al segundo cuatrimestre de 2024:

4.1.1. Evaluación al Sistema de Control Interno.

De acuerdo con la actualización de los activos de información e índice de información clasificada y coordinaciones previas por parte de la Oficina de Control Interno se realiza mesa de trabajo para validación y ajustes de riesgos de seguridad de la Información, así:

- Riesgo 10 – Control 1

Control Actual:

El profesional de la oficina de control interno designado 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 con el requerimiento, como soporte se contara con el correo electrónico, en caso de no contar con solicitud o requerimiento previo se debe solicitar la autorización a la jefatura de control interno, una vez sea autorizada, se debe dejar correo electrónico para efectos de trazabilidad.

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

Ajustes:

Activo: Herramienta de registro y seguimiento Planes de mejoramiento interno

Riesgo: Pérdida de la Integridad.

Amenaza: Corrupción de datos, Indisponibilidad del sistema de información, Mal funcionamiento del software.

Vulnerabilidad: Uso incorrecto de software y hardware.

Consecuencia: Interrupción de los sistemas / procesos

Proyección y ajustes del control:

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.

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

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

El control define "(...) Los responsables de la generación de información (funcionarios públicos y/o contratistas) verifican de forma cuatrimestral la entrega de soportes relacionados con el cumplimiento de metas relacionadas al Plan de Acceso a la Justicia (…)". Asimismo, establece "(…) como evidencia se entrega los soportes de la documentación entregada en los repositorios SharePoint disponibles para el área (...)" (negrilla fuera de texto). idónea para la ejecución del control.

Lo anterior permite identificar que, en la descripción del Control no hay claridad ni especificación de la evidencia de la acción, por lo cual no es posible determinar si el proceso aportó la evidencia.

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

4.1.3. Proceso de Gestión de Emergencias (GE).

- ❖ **Recomendación Riesgo 14 - Control 1: Revisar Descripción del Control.**

Teniendo en cuenta lo definido en el control: "(...) como evidencia se entregan los informes de seguimiento a la operación, informe de interventoría y el informe de supervisión, en caso de no contar con las evidencias del último mes de cada cuatrimestre, estas se cargarán en las evidencias del corte del próximo cuatrimestre (...)" (negrilla y subrayado fuera de texto); esta Oficina observa que, no hay completitud de los soportes allegados por el proceso que den cuenta de la ejecución idónea del control.

Ahora bien, según la Guía de Administración del Riesgo (G-FI-04) de la Entidad: "La definición del control debe incluir en que situaciones se presentan ***desviaciones entre el resultado esperado y el resultado obtenido*** y que acciones se deben tomar si se presentan dichas ***desviaciones***"; por lo cual el ajuste realizado sobre el Control respecto a la variable ***desviación*** no obedece a lo previsto en la citada guía, toda vez que, la misma debe documentarse respecto al resultado y no sobre la evidencia de la acción que se debe allegar como cumplimiento a la ejecución del control.

Lo anterior permite identificar que, en la descripción del Control no hay claridad ni especificación de la evidencia de la acción, por lo cual no es posible determinar si el proceso aportó la evidencia

- Ajustes a Recomendación:

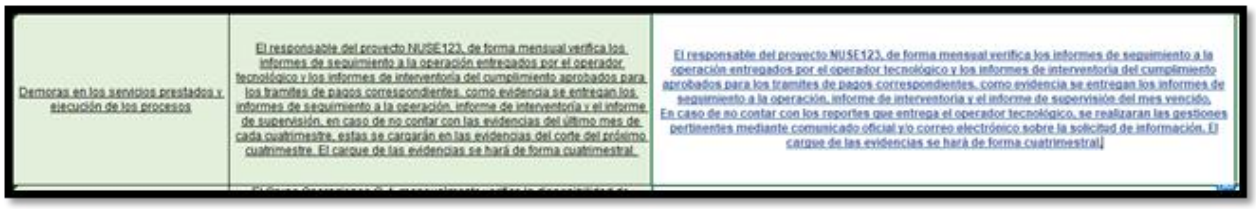
Control Actual:

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, en caso de no contar con las evidencias del último mes de cada cuatrimestre, estas se cargarán en las evidencias del corte del próximo cuatrimestre. El cargue de las evidencias se hará de forma cuatrimestral.

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

Proyección y ajustes del control:

El 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.



Grafica 3. Ajuste a Control.

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

- **Recomendación Riesgo 15 - Control 1: Revisión y Ajustes de evidencias**

Soportes para los meses de mayo, junio, julio y marzo de 2024, en donde se relacionan los Informes técnicos de funcionamiento de las UPS, por parte del Contratista.

Asimismo, la Oficina de Control Interno reitera la recomendación hecha en el Informe del cuatrimestre anterior: (…) se recomienda a la 1LD cargar dentro de las evidencias el Contrato de Mantenimiento suscrito, con el fin de verificar que la ejecución de los mantenimientos a UPS y Planta Eléctrica se realiza con base a la programación establecida”

Teniendo en cuenta lo definido en el control:

"(...) Como evidencia se generan **las actas del contratista del mantenimiento** y los informes técnicos de funcionamiento de las UPS "(negrilla fuera de texto); esta Oficina observa que, no hay completitud de los soportes remitidos por el proceso, toda vez que no se evidencian las actas del contratista de mantenimiento; por lo que, se recomienda allegar los soportes correspondientes.

- ❖ Ajustes a Recomendación:

Control Actual:

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 generan las actas del contratista del mantenimiento y 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.

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

Proyección y ajustes del control:

El 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.

En referencia a la recomendación hecha en el Informe del cuatrimestre anterior: (…) "***se recomienda a la 1LD cargar dentro de las evidencias el Contrato de Mantenimiento suscrito***", para el Centro de Comando, Control, Comunicaciones y Cómputo (C4) no es pertinente esta recomendación y solicitud de información, tomando como referencia que esta oficina no realiza la supervisión y/o el apoyo a la supervisión del contrato de mantenimiento y no se tiene acceso a este contrato, cabe resaltar que en el C4, solo se realiza el seguimiento y monitoreo del funcionamiento de UPS para hacer la solicitud de mantenimientos respectivo y demás requerimientos que comprometen el sistema eléctrico de C-4.

4.1.4. Proceso Gestión de Seguridad y Convivencia (GS).

- **Recomendación Riesgo 23 - Control 1: Revisión y Ajustes de Evidencias.**

Una vez verificados los soportes suministrados por el proceso se identificó que no se allegó la evidencia correspondiente a la ejecución del control, pues en el soporte PDF cargado se manifiesta: "(…) no cuento con evidencias pues la actividad de actualización de esos registros no se ha adelantado este año, considerando que el uso de los datos consignados en el formulario "mercados criminales y aspectos sociales económicos y estructurales", se ha reducido considerablemente luego del cambio de administración. En todo caso, podemos plantear una actualización general para el último cuatrimestre, avanzando también en la redefinición del control, buscando que este se adecue a la realidad del uso actual de esos datos."

Se observa que el proceso no aportó la evidencia idónea y definida para demostrar la ejecución del control, por lo que, se recomienda tanto a la 1LD como a la 2LD validar la descripción del riesgo identificado y el control asociado, toda vez que, para el primer cuatrimestre de la vigencia se presentó una justificación similar por parte del proceso.

- Ajustes a Recomendación:

Control Actual:

El responsable de gestión de la información de la Subsecretaría de seguridad y convivencia garantiza que los registros del formulario sean verificados cuatrimestralmente, esto se evidenciará mediante la tabla de avance de las actualizaciones requeridas a cada localidad durante el periodo. En caso de no realizar la actualización completa, los registros pendientes se sumarán a la meta de actualización del siguiente periodo.

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

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.

Gráfica.4 Ajustes a Control.

4.1.5. Proceso Gestión Tecnologías de Seguridad y Emergencia (GST)

- ❖ Recomendación Riesgo 32 - Control 1: Ajustar Evidencias.

Teniendo en cuenta lo definido en el control: "(...) como evidencia se debe presentar la conciliación técnica mensual provista por la empresa contratista y el responsable del seguimiento (...), en caso de no contar con las conciliaciones técnicas del último mes de cada cuatrimestre, este se cargará en las evidencias del corte del próximo cuatrimestre" (negrilla y subrayado fuera de texto); esta Oficina observa que, no hay completitud de los soportes allegados por el proceso que den cuenta de la ejecución idónea del control.

Ahora bien, según la Guía de Administración del Riesgo (G-FI-04) de la Entidad: “La definición del control debe incluir en que situaciones se presentan desviaciones entre el resultado esperado y el resultado obtenido y que acciones se deben tomar si se presentan dichas desviaciones”; por lo cual el ajuste realizado sobre el Control respecto a la variable desviación no obedece a lo previsto en la citada guía, toda vez que, la misma debe documentarse respecto al resultado y no sobre la evidencia de la acción que se debe allegar como cumplimiento a la ejecución del control.

Por lo anterior, se observa que, como se ha mencionado reiteradamente en los Informes emitidos por la Oficina de Control Interno, el proceso no aporta la evidencia idónea y definida para demostrar la ejecución del control. Asimismo, se sugiere revisar la descripción del control.

- Ajustes a Recomendación:

Control Actual:

El responsable del seguimiento del contrato de mantenimiento de video vigilancia, supervisa los mantenimientos externos a los equipos activos del sistema de video vigilancia, como evidencia se debe presentar la conciliación técnica mensual provista por la empresa contratista y el responsable del seguimiento (Interventoría - supervisión SDSCJ), para los casos de mantenimiento en C-4 (instalaciones C-4 y DataCenter Bomberos), en caso de no contar con las conciliaciones técnicas del último mes de cada cuatrimestre, este se cargara en las evidencias del corte del próximo cuatrimestre. El cargue de las evidencias se hará de forma cuatrimestral.

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

Proyección y ajustes del control:

El 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.

Deficiencias o deterioro del servicio al ciudadano	El responsable del seguimiento del contrato de mantenimiento de video vigilancia, supervisa los mantenimientos externos a los equipos activos del sistema de video vigilancia, como evidencia se debe presentar la conciliación técnica mensual provista por la empresa contratista y el responsable del seguimiento (Interventoría - supervisión SDSCJ), para los casos de mantenimiento en C-4 (instalaciones C-4 y DataCenter Bomberos), en caso de no contar con las conciliaciones técnicas del último mes de cada cuatrimestre, este se cargara en las evidencias del corte del próximo cuatrimestre. El cargue de las evidencias se hará de forma cuatrimestral.	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.

Gráfica.5 Ajustes a Control.

Para esta recomendación, se informa por parte del equipo de trabajo del proceso de Gestión de Emergencias (GE), se realizará el cargue de los informes faltantes según la recomendación de la OCI en el próximo cargue de evidencias del tercer corte de cuatrimestre.

- ❖ Recomendación Riesgo 32 - Control 2: Ajustar Evidencias.

Teniendo en cuenta lo definido en el control: "(...) Las Evidencias corresponde al Informe mensual de la empresa contratista e informe de seguimiento mensual del contrato" (negrilla fuera de texto); esta Oficina observa que, no hay completitud de los soportes allegados por el proceso

Por lo anterior, se observa que el proceso no aportó la evidencia idónea y definida para demostrar la ejecución del control, por lo que, se recomienda allegar los soportes correspondientes

- ❖ Ajustes a Recomendación:

Control Actual:

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 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 corresponde al Informe mensual de la empresa contratista e informe de seguimiento mensual del contrato. El cargue de las evidencias se hará de forma cuatrimestral.

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

Proyección y ajustes del control:

El 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

Para esta recomendación, se informa por parte del equipo de trabajo del proceso de Gestión de Emergencias (GE), se realizará el cargue de los informes faltantes según la recomendación de la OCI en el próximo cargue de evidencias del tercer corte de cuatrimestre.

Documentación Mesas de Trabajo:

Las mesas de trabajo llevadas a cabo por la Dirección de Tecnologías y Sistemas de la Información, en conjunto con las áreas pertinentes, fueron documentadas mediante la elaboración de sus respectivas actas. Estas actas están disponibles para consulta en los repositorios ubicados en la carpeta Share Point:

https://scjgovcol.sharepoint.com/:f:/r/sites/DireccionTIC/Documentos%20compartidos/Gobierno TI/MIPG/Riesgos/Seguridad%20Informaci%C3%B3n/Informes/2024/Tercer%20Cuatrimestre/Actas%20Mesas%20de%20Trabajo?csf=1&web=1&e=9iQq4T

La Dirección de Tecnologías y Sistemas de la Información se permite realizar las siguientes aclaraciones con base a los controles establecidos para los riesgos de seguridad de la Información de acuerdo con las mesas de trabajos realizadas con las áreas, así:

# Riesgo	Proceso	Control	Comentarios
R10-C1	Evaluación al Sistema de Control Interno.	*El profesional de la oficina de control interno designado 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 con el requerimiento, como soporte se contara con el correo electrónico, en caso de no contar con solicitud o requerimiento previo se debe solicitar la autorización a la jefatura de control interno, una vez sea autorizada, se debe dejar correo electrónico para efectos de trazabilidad.*	Se ajusta el control: 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.

# Riesgo	Proceso	Control	Comentarios
R14-C1	Gestión 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, en caso de no contar con las evidencias del último mes de cada cuatrimestre, estas se cargarán en las evidencias del corte del próximo cuatrimestre. El cargue de las evidencias se hará de forma cuatrimestral.*	Se ajusta el control: 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-C1	Gestión 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 generan las actas del contratista del mantenimiento y 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.*	Se ajusta el control: 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.
R21-C1	Proceso Gestión de Seguridad y Convivencia	*El responsable de gestión de la información de la Subsecretaría de seguridad y convivencia garantiza que los registros del formulario sean verificados cuatrimestralmente, esto se evidenciará mediante la tabla de avance de las actualizaciones requeridas a cada localidad durante el periodo. En caso de no realizar la actualización completa, los registros pendientes se sumarán a la meta de actualización del siguiente periodo.*	Se ajusta el Control: 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.

R32-C1	Gestión Tecnologías de Seguridad y Emergencia	El responsable del seguimiento del contrato de mantenimiento de video vigilancia, supervisa los mantenimientos externos a los equipos activos del sistema de video vigilancia, como evidencia se debe presentar la conciliación técnica mensual provista por la empresa contratista y el responsable del seguimiento (Interventoría - supervisión SDSCJ), para los casos de mantenimiento en C-4 (instalaciones C-4 y DataCenter Bomberos), en caso de no contar con las conciliaciones técnicas del último mes de cada cuatrimestre, este se cargara en las evidencias del corte del próximo cuatrimestre. El cargue de las evidencias se hará de forma cuatrimestral.	De acuerdo con el nuevo mapa de procesos, el riesgo y el control previamente suscritos al proceso de Gestión de Emergencias se migran al proceso de Gestión de Tecnologías de Seguridad y Emergencias. Adicionalmente, se realiza un ajuste al control correspondiente: El supervisor del contrato de mantenimiento de video vigilancia y los profesionales de apoyo al mismo, realizan seguimiento a los mantenimientos de los equipos que conforman el sistema de video vigilancia, como evidencia se debe presentar el reporte mensual de los mantenimientos realizados avalado por la interventoría y/o supervisión acompañado de la conciliación técnica mensual de ANS aplicados al contratista, mes vencido, en caso de no contar con los reportes que entrega el contratista, se realizaran las gestiones pertinentes mediante comunicado oficial y/o correo electrónico sobre la información. El cargue de las evidencias se consolidará de forma cuatrimestral.
R32-C2	Gestión Tecnologías de Seguridad y Emergencia	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.	De acuerdo con el nuevo mapa de procesos, el riesgo y el control previamente suscritos al proceso de Gestión de Emergencias se migran al proceso de Gestión de Tecnologías de Seguridad y Emergencias. Adicionalmente, se realiza un ajuste al control correspondiente: 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.

Tabla 2. Controles Gestionados.

4.2. Actualización Riesgos.

En relación con la actualización de la matriz de activos de información y el índice de información clasificada y reservada para la vigencia 2024, así como la clasificación de activos con criticidad alta, se han identificado nuevos riesgos y controles. Estos surgieron a partir de las mesas de trabajo realizadas con las áreas involucradas en los diferentes procesos:

# Riesgo	Proceso	Activo de Información	Control
R3-C1	Acceso y Fortalecimiento a la Justicia.	Bases de datos información operativa de los programas y estrategias DRPA	El Secretario del Centro Especial de Reclusión, registra y valida cuando se requiera las solicitudes de acceso a información archivada, validando previamente que las mismas hayan sido autorizadas por la Dirección del C.E.R a través de memorando y/o correo electrónico; a su vez tendrá a su cargo las llaves del archivador de documentos ubicado en el área administrativa del Centro, en caso de no contar con solicitud o requerimiento previo se debe solicitar esta autorización a la dirección del CER, una vez sea autorizada, se debe dejar este soporte para efectos de trazabilidad, la evidencia se reportara de forma Cuatrimestral.
R4-C1	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	Base de datos del Sistema de información y administración de Bienes SIMBA	El supervisor de contratos valida de forma mensual, que las fallas en la producción de informes de gestión de la plataforma se reporten a través de la mesa de servicio con el fin que este sea escalado al personal encargado de realizar las actualizaciones y/o mejoras al sistema (SIMBA), como evidencia se entrega el reporte mensual de fallas de producción el cual se solicitara mediante correo electrónico y/o comunicado oficial a la DTSI. en caso de no entregar el reporte se debe informar al director de Bienes con las acciones para dar cumplimiento.
R4-C2	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	Base de datos del Sistema de información y administración de Bienes SIMBA	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.	Base de datos del Sistema de información y administración de Bienes SIMBA	El administrador de la plataforma SIMBA, de forma cuatrimestral realiza capacitación y/o sensibilización a funcionarios, contratistas y terceros sobre el correcto uso de la plataforma SIMBA de acuerdo a las funcionalidades y servicios, como soporte de la evidencia se dejará las listas de asistencia y/o soportes documentales de las capacitaciones, para los casos que el personal no asista se reprogramará una nueva sesión de capacitación

R4-C4	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	Base de datos del Sistema de información y administración de Bienes SIMBA	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
R13-C1	Gestión de Comunicaciones Estratégicas.	RRSS - Redes Sociales	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.
R17-C1	Gestión de Emergencias.	Base de datos incidentes SOARS	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.
R18-C1	Gestión de Emergencias.	Bitácora de transferencia de mando área de seguimiento	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.

R30-C1	Gestión Integral a las Personas Privadas de la Libertad - PPL.	Historia de PPL dentro del CER	El Secretario del Centro Especial de Reclusión, registra y valida cuando se requiera las solicitudes de acceso a información archivada, validando previamente que las mismas hayan sido autorizadas por la Dirección del C.E.R a través de memorando y/o correo electrónico; a su vez tendrá a su cargo las llaves del archivador de documentos ubicado en el área administrativa del Centro, en caso de no contar con solicitud o requerimiento previo se debe solicitar esta autorización a la dirección del CER, una vez sea autorizada, se debe dejar este soporte para efectos de trazabilidad, la evidencia se reportara de forma Cuatrimestral

Tabla 3. actualización de Riesgos

Documentación Mesas de Trabajo:

Las mesas de trabajo llevadas a cabo por la Dirección de Tecnologías y Sistemas de la Información, en conjunto con las áreas pertinentes, fueron documentadas mediante la elaboración de sus respectivas actas. Estas actas están disponibles para consulta en los repositorios ubicados en la carpeta Share Point:

https://scjgovcol.sharepoint.com/:f:/r/sites/DireccionTIC/Documentos%20compartidos/Gobierno TI/MIPG/Riesgos/Seguridad%20Informaci%C3%B3n/Informes/2024/Tercer%20Cuatrimestre/Actas%20Mesas%20de%20Trabajo%20Nuevos%20Riesgos?csf=1&web=1&e=TWVbVk

4.3. Matriz de Riesgos de Seguridad de la Información.

Tomando como referencia las actividades de actualización de activos de información vigencia 2024 y 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 y la reestructuración del mapa de procesos de la Entidad, se presentan los ajustes a riesgos y controles 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 Confidencialidad	Los responsables de la generación de información (funcionarios públicos y/o contratistas) verifican de forma cuatrimestral la entrega de soportes relacionados con el cumplimiento de metas relacionadas al Plan de Acceso a la Justicia de acuerdo con la naturaleza de los documentos (mensual - trimestral -semestral y anual) a la Dirección de Acceso a la Justicia. En caso de incumplimiento de la entrega de los documentos en los plazos establecidos, el Director o su equipo delegado de DAJ solicita a los responsables la entrega oportuna de la información, Sopena del incumplimiento de metas, requerimientos internos y externos; como evidencia se entrega los soportes de la documentación entregada en los repositorios SharePoint disponibles para el área.
R2-C1	Acceso y Fortalecimiento a la Justicia	Pérdida de la Confidencialidad	El profesional y/o los profesionales de la dirección de acceso designados para esta actividad trimestralmente solicita la verificación de los permisos de derecho de acceso a los diferentes formularios, de acuerdo con los roles y responsabilidades asignados para tal fin, como soporte de la revisión enviará este profesional comunicación oficial y/o correo electrónico a los responsables del área solicitando esta información, en caso que los usuarios no tengan autorización se retiraran permisos de acceso y se informara de las acciones al Jefe de área.
R3-C1	Acceso y Fortalecimiento a la Justicia	Pérdida de la Integridad	El profesional responsable del reporte de riesgos y controles de Seguridad de la Información debe validar mensualmente la ejecución del plan de copias de respaldo de las bases de datos de la Dirección de Responsabilidad Penal Adolescente (DRPA), asegurando que se cumplan los pasos y plazos establecidos para garantizar la integridad de la información, como evidencia se presenta al director el comunicado oficial y/o correo electrónico sobre la ejecución del plan de copias de respaldo de las bases de datos. En caso de no realizar las actividades establecidas en el plan, se debe informar al director a través de correo electrónico sobre los motivos y las acciones para cumplir con el mismo.
R4-C1	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	Pérdida de la Integridad	El supervisor de contratos valida de forma mensual, que las fallas en la producción de informes de gestión de la plataforma se reporten a través de la mesa de servicio con el fin que este sea escalado al personal encargado de realizar las actualizaciones y/o mejoras al sistema (SIMBA), como evidencia se entrega el reporte mensual de fallas de producción el cual se solicitara mediante correo electrónico y/o comunicado oficial a la DTSI. en caso de no entregar el reporte se debe informar al director de Bienes con las acciones para dar cumplimiento.

# Riesgo	Proceso/Dependencia	Riesgo	Control
R4-C2	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	Pérdida de la Integridad	El administrador de la plataforma SIMBA, realiza solicitud de forma mensual por correo electrónico y/o comunicado oficial a los talleres sobre el cambio de contraseña para la plataforma de acceso (SIMBA) de acuerdo a las funciones habilitadas para cada taller, En caso de no realizar la solicitud dentro de la vigencia del mes se informara al director de bienes los motivos y las acciones para enviar la notificación, como evidencia se entregara la solicitudes de cambio de contraseña a los talleres.
R4-C3	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	Pérdida de la Integridad	El administrador de la plataforma SIMBA, de forma cuatrimestral realiza capacitación y/o sensibilización a funcionarios, contratistas y terceros sobre el correcto uso de la plataforma SIMBA de acuerdo a las funcionalidades y servicios, como soporte de la evidencia se dejará las listas de asistencia y/o soportes documentales de las capacitaciones, para los casos que el personal no asista se reprogramara 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.

# Riesgo	Proceso/Dependencia	Riesgo	Control
R6-C1	Atención y Relación con el Ciudadano.	Pérdida de la Integridad Perdida de Confidencialidad	El responsable del equipo de cobro persuasivo, semestralmente, verifica con el personal de soporte técnico los usuarios activos en el sistema de procesamiento de información de los expedientes de cobro persuasivo de acuerdo a los roles y responsabilidades asignados, como soporte de la revisión enviara correo electrónico y/o comunicación vía Teams solicitando él envió de información y la respuesta requerida al personal encargado, en caso que exista usuarios no autorizados se solicita retirar los permisos de acceso e informar las actividades realizadas.
R7-C1	Control Disciplinario.	Pérdida de la Integridad	El auxiliar administrativo de la oficina de Control Disciplinario interno designado, previa autorización del jefe OCDI, realiza cada vez que se requiera la autorización de acceso a los usuarios a la información, otorgando los permisos de lectura y/o edición de acuerdo al requerimiento, como soporte se contará con la solicitud de permisos a través de correo electrónico, en caso de no contar con solicitud o requerimiento previo no se dará autorización de ingreso a la información.
R8-C1	Control Disciplinario.	Pérdida de la Confidencialidad	El auxiliar administrativo de la oficina de Control Disciplinario Interno asignado, de forma cuatrimestral verifica los permisos de derecho de acceso a los expedientes de Investigaciones Disciplinarios digitales, de acuerdo con los roles y responsabilidades asignados para tal fin, como soporte de la revisión envía comunicación oficial y/o correo electrónico al Jefe de OCDI informando los usuarios que cuentan con acceso y el tipo de acceso a la información, en caso que los usuarios no tengan autorización se retiraran permisos de acceso y se informara de las acciones al Jefe de OCDI.
R9-C1	Direccionamiento Estratégico.	Pérdida de la Disponibilidad	El profesional asignado por la Oficina Asesora de Planeación para las publicaciones en el sitio web trimestralmente realiza el seguimiento y monitoreo a las publicaciones que se deben realizar por cada periodo en el sitio web de la Entidad mediante correo electrónico a los responsables con base al esquema de publicación. En caso de no recepcionar la información para publicación se deberá informar al Jefe de la Oficina de Planeación. Como evidencia quedara el correo de notificación y el esquema de publicación.
R10-C1	Evaluación al Sistema de Control Interno.	Pérdida de la Integridad	El profesional de la Oficina de Control Interno de forma trimestral descarga el reporte del sistema de información con el estado de los planes de mejoramiento institucional y procede a cargar el archivo en el repositorio SharePoint disponible para la Oficina de Control Interno. en caso de no poder descargar el reporte se solicita a la Dirección de Tecnologías y Sistemas de la Información se genere el reporte correspondiente por parte del administrador de la herramienta.

# Riesgo	Proceso/Dependencia	Riesgo	Control
R10-C2	Evaluación al Sistema de Control Interno.	Pérdida de la Integridad	La Jefatura de la Oficina de Control Interno al inicio de cada vigencia solicitara a cada uno de los procesos y/o dependencias por escrito (Correo o Memorando), información de los enlaces responsables del diligenciamiento y reporte del avance del plan de mejoramiento institucional, en caso de no recibir respuesta del proceso y/o dependencias no se le autoriza acceso a la información. como evidencia se presenta el comunicado oficial enviado y las respuestas de los procesos y/o dependencias.
R11-C1	Evaluación al Sistema de Control Interno.	Pérdida de la Integridad	El profesional de la Oficina de Control Interno de forma trimestral descarga el reporte del sistema de información en el que se genere el reporte a los planes de mejoramiento por procesos (internos) y se cargara este archivo en el repositorio SharePoint disponible para la Oficina de Control Interno. en caso de no poder descargar el reporte se solicita a la DTSI se genere el reporte correspondiente por parte del administrador de la herramienta.
R12-C1	Gestión Contractual.	Pérdida de la Disponibilidad Perdida de la Integridad	El responsable del equipo de archivo de la Dirección Jurídica y Contractual anualmente realiza la intervención documental de los expedientes en referencia a la completitud y correspondencia de archivos de los expedientes que se maneja en el área, como evidencia se genera el inventario documental de la DJC. En caso de no entregar el inventario documental a las instancias correspondientes se debe informar al Director(a) Jurídico(a) y Contractual de las acciones para dar cumplimiento.
R13-C1	Gestión de Comunicaciones Estratégicas.	Pérdida de la Confidencialidad y Perdida de la Integridad	El Líder Digital de la Oficina Asesora de Comunicaciones realiza de forma trimestral y/o cuando halla novedades con el personal encargado de las redes sociales, la actualización de las contraseñas de acceso a las diferentes cuentas de redes sociales de la Entidad , como evidencia se debe enviar comunicación oficial y/o correo electrónico al Jefe de la OAC evidenciando el cambio de contraseña, En caso de no realizar la actividad el jefe de la OAC tomará las acciones necesarias para que se ejecute el control, como evidencia se presenta el comunicado oficial enviado por el líder Digital.
R14-C1	Gestión de Emergencias	Pérdida de la Confidencialidad	El responsable del proyecto NUSE123, de forma mensual verifica los informes de seguimiento a la operación entregados por el operador tecnológico y los informes de interventoría del cumplimiento aprobados para los tramites de pagos correspondientes. como evidencia se entregan los informes de seguimiento a la operación, informe de interventoría y el informe de supervisión del mes vencido, En caso de no contar con los reportes que entrega el operador tecnológico, se realizaran las gestiones pertinentes mediante comunicado oficial y/o correo electrónico sobre la solicitud de información. El cargue de las evidencias se hará de forma cuatrimestral.

# Riesgo	Proceso/Dependencia	Riesgo	Control
R14-C2	Gestión de Emergencias	Perdida de la Integridad	El Grupo Operaciones C-4, mensualmente verifica la disponibilidad de personal asignado para el cumplimiento de las tareas dentro de la operación del NUSE123, de lo cual entregara una proyección sobre ausencia de personal y necesidades de operación. como evidencia se entregará matriz proyección de turnos operación de C4, para toma de decisiones. en caso de no contar con el personal necesario de operación envían un correo al jefe de C4, con la novedad.
R14-C3	Gestión de Emergencias	Pérdida de la Disponibilidad	El grupo de entrenamiento C-4, semestralmente, realiza capacitación y /o sensibilización a funcionarios y contratistas sobre el correcto uso de contraseñas de acuerdo a lo establecido en el manual de seguridad y privacidad de la información de la Entidad, como soporte de la evidencia se dejarán las listas de asistencia y documentos de apoyo de las capacitaciones, para los casos que personal no asista se procede con la reprogramación de una nueva sesión de capacitación.
R15-C1	Gestión de Emergencias	Pérdida de la Disponibilidad	El grupo de seguimiento de infraestructura tecnológica del C-4, realizan la verificación de acciones preventivas y correctivas a UPS y Planta eléctrica programados en el contrato de mantenimiento establecido por parte de la Secretaría Distrital de Seguridad, convivencia y Justicia. Como evidencia se cargan los informes técnicos de funcionamiento de las UPS, en caso de no realizar los mantenimientos programados se deberá informar mediante correo electrónico sobre los motivos, así como las acciones para cumplir con los mantenimientos. el cargue de evidencia se hará trimestralmente.
R16-C1	Gestión de Emergencias	Pérdida de Confidencialidad, Integridad y/o disponibilidad de la información	El jefe del C4 delega a la empresa contratista el mantenimiento y operación del sistema de comunicaciones. Estas actividades se registran en informes de gestión de la empresa contratista recibidos de forma mensual evidenciando la operación del sistema de comunicaciones controlada por ANS, que en caso de estar por debajo de umbral se penaliza económicamente. las Evidencia corresponde al Informe mensual de la empresa contratista. El cargue de las evidencias se hará trimestralmente.
R17-C1	Gestión de Emergencias	Pérdida de la Disponibilidad.	El coordinador de la Sala SOARS, realiza de forma mensual el cargue de la copia de seguridad de la base de datos incidentes SOARS en el repositorio establecidos en el C-4, en caso de no realizar la copia de seguridad se debe informar al jefe de C-4 los motivos y las acciones para el cargue de esta información, como evidencia se envía correo electrónico y/o comunicado oficial al líder del C-4.

# Riesgo	Proceso/Dependencia	Riesgo	Control
R18-C1	Gestión de Emergencias	Pérdida de la Disponibilidad	El coordinador de la Sala SOARS, realiza de forma mensual el cargue de la copia de seguridad de la bitácora de transferencia de mando del área de seguimiento en el repositorio establecidos en el C-4, en caso de no realizar la copia de seguridad se debe informar al jefe de C-4 los motivos y las acciones para el cargue de esta información, como evidencia se envía correo electrónico y/o comunicado oficial al líder del C-4.
R19-C1	Gestión de Seguridad y Convivencia	Pérdida de Confidencialidad	El responsable de almacenamiento de las actas debe asegurar que los permisos otorgados a los usuarios sobre estos documentos, sean actualizados y/o retirados semestralmente, de acuerdo con los roles y permisos de cada funcionario que accede a la información, debe quedar como evidencia correo electrónico enviado al líder del proceso evidenciando los funcionarios que tienen acceso y el tipo de permiso que tienen (lectura, escritura, o ambos) En caso de que el responsable de almacenamiento de las actas no tenga permisos de gestión sobre la carpeta, deberá solicitarlos al secretario.
R20-C1	Gestión de Seguridad y Convivencia	Pérdida 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	Pérdida 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.

# Riesgo	Proceso/Dependencia	Riesgo	Control
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 mediante la tabla de verificación de correspondencia de registros. En caso de no cumplir con el porcentaje establecido se requerirá por correo electrónico a los responsables de las actividades para realizar la verificación respectiva.
R25-C1	Gestión de Tecnología de Información	Pérdida de Confidencialidad, integridad y/o disponibilidad de la información	El responsable de sistema de información y/o infraestructura Tecnológica verifica de forma cuatrimestral el seguimiento al plan de trabajo de versionamiento de los ambientes de pruebas y productivos asociados a los sistemas de información, en caso de no realizar el seguimiento se debe evidenciar las causas de no realizar las actividades del plan a través de actas, informes y/o correos electrónicos, como evidencia de la ejecución del control se contara con los avances de las actividades del plan mediante bitácoras de actividades, actas y/o comunicado oficial.

# Riesgo	Proceso/Dependencia	Riesgo	Control
R25-C2	Gestión de Tecnología de Información	Pérdida de Confidencialidad, integridad y/o disponibilidad de la información	El responsable de sistema de información realiza seguimiento cuatrimestral a la ejecución del plan de actualización documental de la arquitectura de los sistemas de información, en caso de no contar con el seguimiento trimestral al plan de actualización documental de la arquitectura, se deberá contar con los manuales técnicos actualizados de cada uno de los sistemas de información. Como evidencia de la ejecución del control se contará con el reporte de seguimiento al plan o con los manuales técnicos de los sistemas
R26-C1	Gestión de Tecnología de Información	Pérdida de Confidencialidad, integridad y/o disponibilidad de la información	El responsable de infraestructura define el mecanismo seguro y estandarizado para la gestión segura de credenciales de administración en la infraestructura tecnológica, así como el seguimiento trimestral al cumplimiento de los mecanismos establecidos, en caso de no contar con el seguimiento trimestral a los mecanismos establecidos, se contará con comunicación formal al Director de Tecnologías informando las alternativas adoptadas. Como evidencia de la ejecución del control se contará con el mecanismo de gestión segura de contraseñas o comunicado formal.
R26-C2	Gestión de Tecnología de Información	Pérdida de Confidencialidad, integridad y/o disponibilidad de la información	El responsable de infraestructura tecnológica realiza seguimiento trimestral al funcionamiento de herramientas de seguridad informática que protegen la información de la SDSCJ, en caso de no hacer seguimiento al funcionamiento se contara con comunicación formal al Director de Tecnologías informando las alternativas adoptadas. Como evidencia de la ejecución del control se contará con el reporte de rendimiento de la infraestructura de seguridad o el comunicado formal.
R27-C1	Gestión Estratégica del Talento Humano.	Pérdida de la Integridad	El Profesional especializado responsable de nómina, solicita a la DTSI en caso de una novedad, el permiso y/o retiro de acceso de usuarios autorizados de forma permanente al sistema de información y/o repositorios asignados para el manejo de esta información, como evidencia se tendrán las comunicaciones de solicitud y/o retiro de acceso de usuarios. en caso de que los permisos no sean gestionados correctamente se reitera la solicitud mediante correo electrónico a la mesa de servicio con los ajustes requeridos. El cargue de evidencia se realizará de forma cuatrimestral.
R28-C1	Gestión Estratégica del Talento Humano.	Pérdida de la Confidencialidad	La Dirección de Gestión Humana define el acceso de los usuarios autorizados y el equipo de archivo de la DGH, controlará el acceso al repositorio de historias laborales para la consulta y manejo de esta documentación, en caso de que los usuarios no cuenten con la autorización de acceso, no se permitirá la consulta a dichos expedientes, como evidencia se tendrá la base de préstamos de historias laborales. el cargue de evidencia se realizará Semestralmente

# Riesgo	Proceso/Dependencia	Riesgo	Control
R29-C1	Gestión Financiera.	Pérdida de la Integridad	El responsable de las áreas que componen la dirección financiera (Presupuesto, Pago y contabilidad) informa al director financiero cada vez que se requiera las solicitudes respecto a los permisos de acceso y/o cancelación de usuarios al aplicativo donde se registra la información financiera, para que se realice la gestión ante la Dirección de tecnologías de la Información, en caso de que los usuarios no cuenten con la autorización de acceso, no se permitirá la consulta a dicha información, como evidencia se tendrá los comunicados oficiales y/o correo electrónicos de las solicitudes de acceso y/o cancelación de usuarios.
R30-C1	Gestión Integral a las Personas Privadas de la Libertad - PPL.	Pérdida de la Disponibilidad Perdida de Confidencialidad	El Secretario del Centro Especial de Reclusión, registra y valida cuando se requiera las solicitudes de acceso a información archivada, validando previamente que las mismas hayan sido autorizadas por la Dirección del C.E.R a través de memorando y/o correo electrónico; a su vez tendrá a su cargo las llaves del archivador de documentos ubicado en el área administrativa del Centro, en caso de no contar con solicitud o requerimiento previo se debe solicitar esta autorización a la dirección del CER, una vez sea autorizada, se debe dejar este soporte para efectos de trazabilidad, la evidencia se reportara de forma Cuatrimestral
R31-C1	Gestión Jurídica.	Pérdida de la Disponibilidad Perdida de la Confidencialidad Perdida de la Integridad	El responsable del equipo de archivo de la Dirección Jurídica y Contractual anualmente realiza la intervención documental de los expedientes en referencia a la completitud y correspondencia de archivos de los expedientes que se maneja en el área, como evidencia se genera el inventario documental de la DJC. En caso de no entregar el inventario documental a las instancias correspondientes se debe informar al Director(a) Jurídico(a) y Contractual de las acciones para dar cumplimiento.
R32-C1	Gestión Tecnológica de Seguridad y Emergencias.	Pérdida de Confidencialidad, Integridad y/o disponibilidad de la información	El supervisor del contrato de mantenimiento de video vigilancia y los profesionales de apoyo al mismo, realizan seguimiento a los mantenimientos de los equipos que conforman el sistema de video vigilancia, como evidencia se debe presentar el reporte mensual de los mantenimientos realizados avalado por la interventoría y/o supervisión acompañado de la conciliación técnica mensual de ANS aplicados al contratista, mes vencido, en caso de no contar con los reportes que entrega el contratista, se realizaran las gestiones pertinentes mediante comunicado oficial y/o correo electrónico sobre la información. El cargue de las evidencias se consolidará de forma cuatrimestral.

# Riesgo	Proceso/Dependencia	Riesgo	Control
R32-C2	Gestión Tecnológica de Seguridad y Emergencias.	Pérdida de Confidencialidad, Integridad y/o disponibilidad de la información	El jefe del C4 supervisa a la empresa contratista del mantenimiento del sistema de video vigilancia y garantías extendidas del Centro de Computo. Estas actividades se registran en los informes de gestión de la empresa contratista, los cuales son recibidos y estos a su vez evidencian la operación del sistema de video vigilancia controlada por ANS, que en caso de estar por debajo de umbral se penaliza económicamente. Las evidencias corresponden al Informe mensual de la empresa contratista e informe de seguimiento mensual del contrato que se allega al mes vencido. El cargue de las evidencias se hará de forma cuatrimestral.
R33-C1	Gestión y Análisis de la Información.	Pérdida de la Integridad	El Profesional Universitario, Especializado y/o Contratista de la Oficina de Análisis de Información y Estudios Estratégicos responsable de la bodega de datos valida mensualmente que la carga de información de las fuentes haya finalizado exitosamente por medio de consultas SQL en el rango de fechas actualizado; cuyo resultado es evidenciado en el indicador de gestión "cumplimiento en la actualización de la bodega de datos" el cual es reportado periódicamente en el Portal MIPG. En caso de incumplimiento de este indicador se deberá realizar la justificación pertinente en el Portal MIPG. Como evidencias se adjunta la consulta SQL y el cargue en el portal MIPG del indicador de gestión asociado.

Tabla 4. Matriz Riesgos de Seguridad de la Información.

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

https://scj.gov.co/es/transparencia/planeacion-presupuesto-ingresos/plan-accion

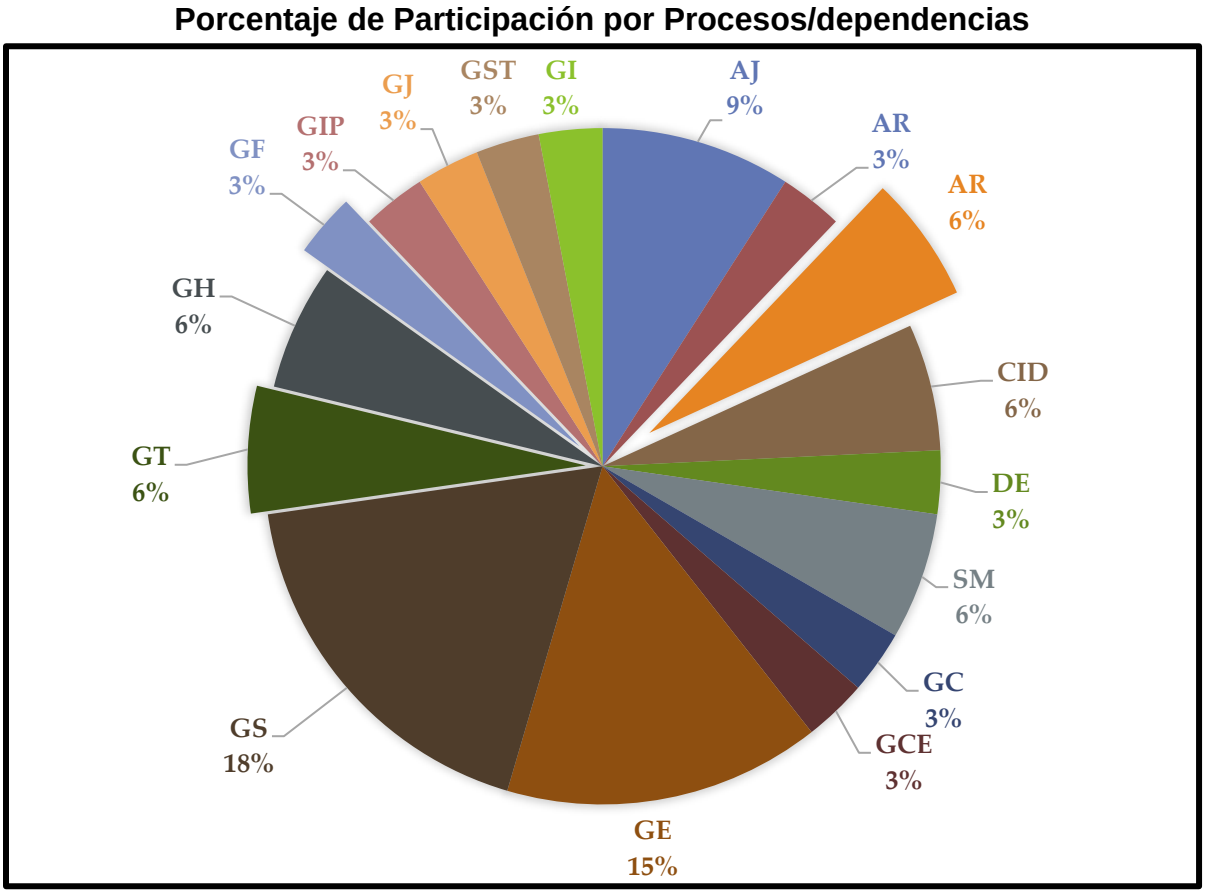
5. ANALISIS DE LA MATRIZ DE RIESGOS

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

PROCESO	SIGLA	RIESGOS
Acceso y Fortalecimiento a la Justicia	**AJ**	**3**
Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	**AB**	**1**
Atención y Relación con el Ciudadano.	**AR**	**2**
Control Disciplinario.	**CID**	**2**
Direccionamiento Estratégico.	**DE**	**1**
Evaluación al Sistema de Control Interno.	**SM**	**2**

Gestión Contractual	**GC**	**1**
Gestión de Comunicaciones Estratégicas.		**1**
Gestión de Emergencias	**GE**	**5**
Gestión de Seguridad y Convivencia	**GS**	**6**
Gestión de Tecnología de Información	**GT**	**2**
Gestión Estratégica del Talento Humano.	**GH**	**2**
Gestión Financiera.	**GF**	**1**
Gestión Integral a las Personas Privadas de la Libertad - PPL.	**GIP**	**1**
Gestión Jurídica	**GJ**	**1**
Gestión Tecnológica de Seguridad y Emergencias.	**GST**	**1**
Gestión y Análisis de Información	**GI**	**1**
	Total Riesgos	**33**

Tabla 5. Análisis Matriz Riesgos.



Grafica 6. Porcentaje Participación.

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%

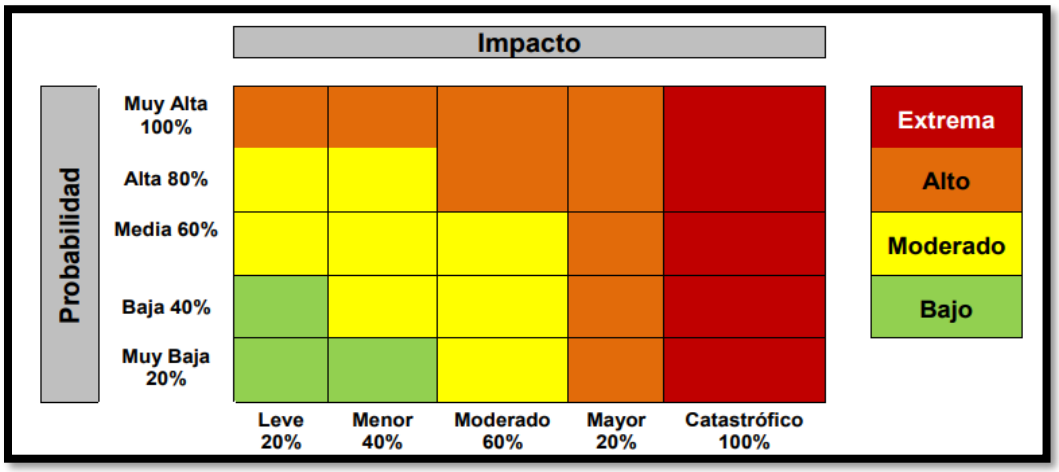
Grafica 7. Fuente: Política de Administración de Riesgos SDSCJ.

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 8. Fuente: Política de Administración de Riesgos SDSCJ.

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



Grafica 9. Fuente: Política de Administración de Riesgos SDSCJ.

Todas las valoraciones se realizaron de parte de los Líderes de proceso o los Líderes Operativos en compañía de sus grupos de trabajo, contando con el acompañamiento y orientación de la Dirección de Tecnologías y Sistemas de la Información, dichas valoraciones de Probabilidad e Impacto nos dan como resultado la Zona de Riesgo Inherente resultado que se detalla 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	2	1	4
Atención y Relación con el Ciudadano (AR)			2		2
Control Disciplinario (CID)			2		2
Direccionamiento Estratégico. (DE)		1			1
Evaluación al Sistema de Control Interno (SM)			3		3
Gestión Contractual (GC)			1		1
Gestión de Comunicaciones Estratégicas. (GCE)			1		1
Gestión de Emergencias (GE)			7		7
Gestión de Seguridad y Convivencia (GS)			7		7
Gestión de Tecnología de Información (GT)		4			4
Gestión Estratégica del Talento Humano (GH)			2		2
Gestión Financiera. (GF)			1		1
Gestión Integral a las Personas Privadas de la Libertad - PPL. (GIP)			1		1
Gestión Jurídica (GJ)			1		1
Gestión Tecnológica de Seguridad y Emergencias. (GST)			2		2
Gestión y Análisis de Información (GI)		1			1
Total	**0**	**7**	**34**	**2**	**43**

Tabla 6. Valoración de Riesgos.

Dada la necesidad de dar trámite y continuidad a los procedimientos y actividades establecidos por los procesos, para ninguno de los riesgos identificados se determinó “Evitar” como medida de tratamiento para el riesgo. Contrario a ello se optó por “Reducir el riesgo” como la medida por los procesos, con esto se hace necesaria la ejecución de controles para minimizar posibilidad de materialización de los riesgos, en concordancia con lo establecido en la Política de Administración de Riesgos de la Entidad.

A continuación, se presenta la cantidad de riesgos y controles por proceso, aclarando que el número de controles no garantiza que el riesgo se materialice o no. Los controles han sido definidos según el criterio de cada proceso y los recursos disponibles, con el objetivo de prevenir su posible ocurrencia.

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

Tabla 7. Riesgos vs Controles.

Desde la Dirección de Tecnologías y Sistemas de la Información se dio acompañamiento a todos los procesos para el cumplimiento de los anteriores parámetros permitiendo un cumplimiento global de todos los controles establecidos, lo que permite una apropiada gestión del riesgo.

El resultado de la gestión del riesgo con base en la ejecución de controles se puede apreciar a detalle en el siguiente cuadro comparativo de la Zona de Riesgo Inherente a la zona de Riesgo Residual:

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	2	1					4
Atención y Relación con el Ciudadano (AR)			2						2
Control Disciplinario (CID)			2						2
Direccionamiento Estratégico. (DE)		1							1
Evaluación al Sistema de Control Interno (SM)			3						3
Gestión Contractual (GC)			1						1
Gestión de Comunicaciones Estratégicas. (GCE)			1						1
Gestión de Emergencias (GE)			7						7
Gestión de Seguridad y Convivencia (GS)			7						7
Gestión de Tecnología de Información (GT)		4							4
Gestión Estratégica del Talento Humano (GH)			2						2
Gestión Financiera. (GF)			1						1
Gestión Integral a las Personas Privadas de la Libertad - PPL. (GIP)			1						1
Gestión Jurídica (GJ)			1						1
Gestión Tecnológica de Seguridad y Emergencias. (GST)			2						2
Gestión y Análisis de Información (GI)		1							1
Total	**0**	**7**	**34**	**2**		**0**	**0**	**0**	**43**

Tabla 8. Riesgo Inherente vs Riesgo Residual.

6. CARGUE EVIDENCIAS

Mediante memorando interno 3-2024-42215 de fecha 12/12/2024 – DTSI, se realizó solicitud de cargue de información para el tercer cuatrimestre de la vigencia 2024, tomando como referencia la información generada en el informe de seguimiento a controles asociados a los riesgos de seguridad de información del segundo cuatrimestre de 2024 generado por la Oficina de Control Interno, donde se entrega información referente a los ajustes de entrega de evidencia por parte de los procesos y áreas para la presente vigencia.

La Política de Administración de Riesgos menciona la realización del seguimiento de la ejecución de los controles de seguridad de la información estructurados para todos los procesos de forma cuatrimestral. Para ello se puso a disposición de los líderes Operativos la Carpeta "*GobiernoTI/MIPG/Riesgos/SeguridadInformación*" en los repositorios SharePoint de la Entidad para el cargue de las evidencias correspondientes a la ejecución de los 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/2024?csf=1&web=1&e=07ebjk

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

Sigla	Proceso	N° Riesgos	N° Controles	Evidencias publicadas controles	% de riesgos cubierto
AJ	Acceso y Fortalecimiento a la Justicia	**3**	**3**	**7**	100%
AB	Administración de Bienes Muebles e Inmuebles para el Fortalecimiento de las Capacidades Operativas.	**1**	**4**	**14**	100%
AR	Atención y Relación con el Ciudadano	**2**	**2**	**10**	100%
CID	Control Disciplinario	**2**	**2**	**3**	100%
DE	Direccionamiento Estratégico.	**1**	**1**	**6**	100%
SM	Evaluación al Sistema de Control Interno	**2**	**3**	**5**	100%
GC	Gestión Contractual	**1**	**1**	**1**	100%
GCE	Gestión de Comunicaciones Estratégicas.	**1**	**1**	**2**	100%
GE	Gestión de Emergencias	**5**	**7**	**36**	100%
GS	Gestión de Seguridad y Convivencia	**6**	**7**	**13**	100%
GT	Gestión de Tecnología de Información	**2**	**4**	**15**	100%
GH	Gestión Estratégica del Talento Humano	**2**	**2**	**7**	100%
GF	Gestión Financiera.	**1**	**1**	**3**	100%
GIP	Gestión Integral a las Personas Privadas de la Libertad - PPL.	**1**	**1**	**1**	100%
GJ	Gestión Jurídica	**1**	**1**	**1**	100%
GST	Gestión Tecnológica de Seguridad y Emergencias.	**1**	**2**	**11**	100%
GI	Gestión y Análisis de Información	**1**	**1**	**8**	100%
	Total	**33**	**43**	**143**	**100%**

Tabla 9. Soporte de Controles.

Esto indica que los líderes de los procesos cumplieron adecuadamente con la entrega de las evidencias que respaldan la ejecución de los controles, conforme a los soportes proporcionados.

De esta manera, se ratifica la destacada gestión llevada a cabo en términos generales por los procesos de la Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ relacionado a la Administración y Gestión de los Riesgos de Seguridad de la Información.

7. CONCLUSIONES

En resumen, al cierre del tercer cuatrimestre de 2024, la Dirección de Tecnologías y Sistemas de la Información reafirma su compromiso y participación mediante la supervisión y monitoreo de los controles asociados a los riesgos de seguridad de la información. Esta labor se lleva a cabo en cumplimiento de la Política de Administración de Riesgos y de los lineamientos establecidos 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), con el respaldo constante de los líderes operativos de cada proceso.

Durante el tercer cuatrimestre de 2024, el monitoreo de los riesgos de seguridad de la información, conforme a los procesos establecidos, evidenció una gestión efectiva que ha favorecido la continuidad operativa y el cumplimiento de los objetivos propuestos. Esta gestión ha sido clave para el fortalecimiento de las actividades y el avance en el cumplimiento de los objetivos de la Entidad en materia de seguridad de la información.

Tras llevar a cabo mesas de trabajo con las áreas correspondientes, en respuesta al informe de seguimiento de la Oficina de Control Interno (OCI) mediante el radicado 3-2024-34703 “Informe de Seguimiento a Controles asociados a los Riesgos de Seguridad de la Información correspondiente al segundo cuatrimestre de 2024” de fecha 21/10/2024 se ha logrado un avance significativo en la revisión de las observaciones señaladas. Esto ha permitido una evaluación más precisa de los controles sugeridos. Asimismo, se destaca el compromiso y la colaboración de todas las áreas involucradas en la implementación de las mejoras propuestas y en el fortalecimiento de la efectividad de los controles.

En referencia a la actualización de los activos de información, establecida en la Política de Administración de Riesgos de la Entidad como un componente fundamental en la identificación, valoración, asignación, control y seguimiento de los riesgos de seguridad de la información que puedan afectar el desarrollo de los procesos y, por ende, el cumplimiento de los objetivos estratégicos para la vigencia 2024, se validaron un total de 322 activos de información, el personal responsable de cada proceso evaluó estos activos conforme a los principios de Confidencialidad, Integridad y Disponibilidad de información. De esta evaluación, se determinó que 71 activos fueron clasificados con una valoración de criticidad Alta, 154 activos con una valoración de criticidad Media y 97 activos con una valoración de criticidad Baja.

Es importante destacar que la Dirección de Tecnologías y Sistemas de la Información encabeza la efectiva implementación de la Política de Administración de Riesgos en lo relacionado con los Riesgos de Seguridad de la Información. Este trabajo se realiza con el apoyo de la Oficina Asesora de Planeación y el respaldo de la Oficina de Control Interno, en estrecha coordinación con los líderes operativos de cada proceso. Gracias a este esfuerzo conjunto, la política se está aplicando y adoptando correctamente durante el período vigente en la Entidad.

Se resalta el compromiso y dedicación de los Líderes de Proceso, Líderes Operativos y sus equipos en la efectiva implementación de los controles asociados a los riesgos de seguridad de la información. Por esta razón, desde la Dirección de Tecnologías y Sistemas de la Información, expresamos nuestro sincero agradecimiento y reconocimiento a todos los colaboradores que hicieron posible el cumplimiento de la meta de seguimiento y carga de evidencias durante el tercer cuatrimestre de 2024.

La Dirección de Tecnologías y Sistemas de la Información, en su compromiso con la mejora continua de la gestión de los riesgos de seguridad de la información durante la vigencia 2024, ratifica su responsabilidad de proporcionar el apoyo metodológico necesario frente a cualquier cambio o ajuste en las caracterizaciones, procedimientos y documentación que sustentan la gestión de cada proceso. Esto incluye la posibilidad de actualizar los riesgos o controles actualmente identificados, garantizando así una gestión efectiva y adaptada a las necesidades de la Entidad.