ALCALDÍA MAYOR DE BOGOTÁ
SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA
AL RESPONDER CITAR EL NR.
Nro. Rad: 3-2024-16877
Fecha: 16/05/2024 04:11:20 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 PRIMER 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, así como siguiendo las directrices establecidas por el Departamento Administrativo de la Función Pública, de forma respetuosa se envía el informe cuatrimestral adjunto al presente documento sobre Riesgos de Seguridad de la Información. Este informe tiene como finalidad su revisión y socialización dentro de su área de responsabilidad.

Agradecemos de antemano sus consideraciones y comentarios al respecto.

Quedamos a su disposición para cualquier aclaración o consulta adicional.

Cordialmente,

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
EDWIN CASTILLO ORTIZ-DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION
FRANCISCO ALFORD BOJACA-COBRO PERSUASIVO
LUIS CARLOS GOMEZ CAMARGO-EQUIPO ATENCION AL CIUDADANO
CLAUDIA XIMENA HORMAZA LOZANO-EQUIPO ATENCION AL CIUDADANO

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

MARY LIZETH BUITRAGO SIERRA-OFICINA ASESORA DE PLANEACION
JOHN ALEXANDER HINCAPIE RUEDA-OFICINA ASESORA DE PLANEACION
DONNYS DEVANES TORRES LOZANO-OFICINA ASESORA DE PLANEACION
ANDRES ORLANDO TORRES EUSSE-OFICINA DE CONTROL INTERNO
YAIDE YAMILE ACEVEDO SARMIENTO-OFICINA DE CONTROL DISCIPLINARIO INTERNO
JENNIFER CATHERINE VELASQUEZ-OFICINA DE CONTROL DISCIPLINARIO INTERNO
SAYRA GUINETTE ALDANA HERNANDEZ-OFICINA DE ANÁLISIS DE INFORMACION Y ESTUDIOS ESTRATEGICOS
DIANA MARCELA FLECHAS RUIZ-OFICINA DE ANÁLISIS DE INFORMACION Y ESTUDIOS ESTRATEGICOS
ADA LUZ SANDOVAL HERAZO-OFICINA CENTRO COMANDO, CONTROL, COMUNICACIONES Y COMPUTO C-4
EDITH NATHALIE ROMERO BARRERA-OFICINA CENTRO COMANDO, CONTROL, COMUNICACIONES Y COMPUTO C-4
ALEXANDER PALACIOS PALACIOS-OFICINA CENTRO COMANDO, CONTROL, COMUNICACIONES Y COMPUTO C-4
ALBERTO SANCHEZ GALEANO-SUBSECRETARIA DE SEGURIDAD Y CONVIVENCIA
SANDRA MILENA PEREZ RAMIREZ-SUBSECRETARIA DE SEGURIDAD Y CONVIVENCIA
ESTEFANIA ESTRADA VILLADA-SUBSECRETARIA DE SEGURIDAD Y CONVIVENCIA
LINA MARIA TORO TAMAYO.-SUBSECRETARIA DE ACCESO A LA JUSTICIA
VIVIANA PAOLA RODRIGUEZ RODRIGUEZ-SUBSECRETARIA DE ACCESO A LA JUSTICIA
EDWIN DARIO MORA GOMEZ-DIRECCION DE ACCESO A LA JUSTICIA
SANDRA PATRICIA PINILLA MARTINEZ-DIRECCION DE GESTION HUMANA
ELIZABETH LESMES ARANDA-DIRECCION DE GESTION HUMANA
ANA MARIA MORENO GARCIA-DIRECCION JURIDICA Y CONTRACTUAL
ANDREA DEL PILAR ROJAS ALVAREZ-DESPACHO SECRETARIO DE SEGURIDAD
Anexos: 1

Elaboró: DIEGO MAURICIO USME GONZALEZ-DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION
Revisó: JAIRO ALONSO BOHORQUEZ BLANCO-DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION |
Aprobó: IVAN HERSAYN PINILLA HERRERA-DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION

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

INFORME PRIMER CUATRIMESTRE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN - 2024

Dirección de Tecnologías y Sistemas de la Información.

Mayo de 2024

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. 1), 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, "*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 primer cuatrimestre de la vigencia 2024.

El monitoreo a la matriz de riesgos de seguridad de información se fundamenta en el trabajo previo de levantamiento de activos de información, donde se validaron un total de 331 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 79 activos fueron clasificados con una valoración de criticidad Alta, 164 activos con una valoración de criticidad Media y 88 activos con una valoración de criticidad Baja.

Sobre el ejercicio de levantamiento de riesgos de seguridad de la información se tomaron como referencia los 79 activos de información clasificados con una valoración de criticidad Alta, siendo aprobados en las actividades previas de levantamiento de activos, de lo cual se validaron y estructuraron mediante acta de reunión un total de 28 riesgos y se generaron 36 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:

1. Atención y Relación con el Ciudadano. (AR)
2. Fortalecimiento Institucional (FI)
3. Gestión de Tecnología de la Información (GT).
4. Gestión y Análisis de la Información (GI).
5. Gestión Estratégica del Talento Humano (GH).

MISIONALES:

6. Acceso y Fortalecimiento a la Justicia (AJ)
7. Gestión de Emergencia (GE)
8. Gestión de Seguridad y Convivencia (GS)

APOYO:

9. Gestión Jurídica (GJ)
10. Gestión Contractual (GC)

SEGUIMIENTO:

11. Evaluación al Sistema de Control Interno (SM)
12. Control Disciplinario (CID)

En líneas generales, cada uno de los procesos y áreas mencionadas ha detectado al menos un riesgo, y todos ellos están en conformidad con los lineamientos establecidos en la Política de Administración de Riesgos PO-FI-02 Ver. 1 adoptada por la SDSCJ. Dicha política está alineada con las directrices establecidas en la "Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 6 - noviembre de 2022" del Departamento Administrativo de la Función Pública – DAFP.

2. 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 realizó para el mes de marzo, el diseño y presentación de pieza gráfica sobre “Seguimiento a riesgos de seguridad de la información” mediante difusión masiva para toda la Entidad. Las evidencias 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/Primer%20Cuatrimestre/Comunicaciones%20Electronicas?csf=1&web=1&e=ZDLGJG

Gráfica.1 Elaboración Uso y Apropiación DTSI.

De otro lado se realizó por parte de la DTSI, memorando electrónico digital 3-2024-12538 de fecha 08/04/2024 – 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 enero, febrero, marzo y abril (Primer Cuatrimestre vigencia 2024) para los procesos y áreas definidas, en el siguiente enlace:

https://scjgovcol.sharepoint.com/:f:/r/sites/DireccionTIC/Documentos%20compartidos/GobiernoTI/MIPG/Riesgos/Seguridad%20Informaci%C3%B3n/Informes/2024/Primer%20Cuatrimestre/Memorando%203-2024-12538?csf=1&web=1&e=0aACzq

Así mismo, se realizó 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 primer 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 tercer cuatrimestre 2023, 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/Primer%20Cuatrimestre/Comunicaciones%20Electronicas?csf=1&web=1&e=ZDLGJG

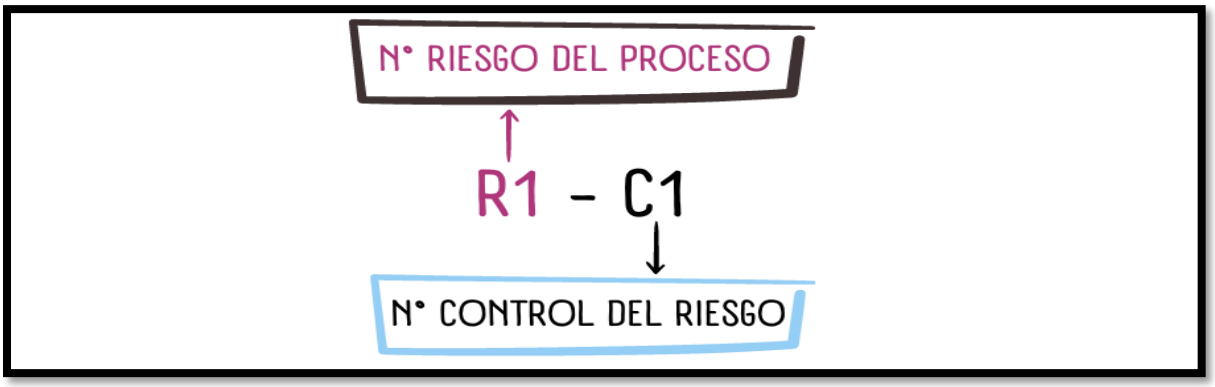
3. MATRIZ DE RIESGOS DE SEGURIDAD DE INFORMACIÓN

Para el primer 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 con la agrupación de la información de los Riesgos de todos los procesos con la información de la Hoja de resumen, listado de activos, Riesgo Inherente, Tratamiento del Riesgo, Valoración con controles y Tratamiento de riesgo residual.
- Todos los Riesgos y controles cumplen con la metodología establecida en la Política de Administración de Riesgos.
- La nomenclatura de cada riesgo corresponde a razón de lo siguiente:



Grafica 2. Elaboración propia

2.1. Recomendaciones OCI.

En referencia a las conclusiones y recomendaciones generadas por la Oficina de Control Interno (OCI) mediante el radicado 3-2024-7270 “Informe de Seguimiento a Controles asociados a los Riesgos de Seguridad de la Información”, se realizaron mesas de trabajo con las áreas, para efectuar la validación de las observaciones emitidas por la Oficina de Control Interno sobre la evaluación de los controles presentados en el tercer cuatrimestre de la vigencia 2023:

En primera instancia se realizó una mesa de trabajo con todas las áreas y procesos para la entrega de información sobre la atención de las observaciones de la Oficina de Control Interno de la Entidad y el seguimiento a los controles de los riesgos de seguridad de la información para la vigencia del primer cuatrimestre de 2024. Además, se solicita información adicional a las áreas y/o procesos que requieran realizar cambios y/o gestiones sobre los controles y riesgos que se deban considerar o tratar en mesas de trabajo posteriores para ajustar la matriz de seguridad de información de la presente vigencia. No se recibieron solicitudes adicionales a las observaciones establecidas por la Oficina de Control Interno. La evidencia de esta mesa de trabajo se encuentra en el siguiente enlace:

https://scjgovcol.sharepoint.com/:b:/r/sites/DireccionTIC/Documentos%20compartidos/GobiernoTI/MIPG/Riesgos/Seguridad%20Informaci%C3%B3n/Informes/2024/Primer%20Cuatrimestre/Actas%20Mesa%20Trabajo/00.%20Acta%20Riesgos%20Seguridad%20Informaci%C3%B3n%2005042024.pdf?csf=1&web=1&e=fNpOkF

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

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

Para esta recomendación, se informó por parte del equipo de trabajo del proceso Acceso y Fortalecimiento a la Justicia (AJ), que se realizará el cargue de las evidencias solicitadas por la OCI, al igual se establece que en el cargue de evidencias del primer cuatrimestre

de riesgos de seguridad de Información se presentará de acuerdo con las recomendaciones de la OCI.

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

Para esta recomendación, se informó por parte del equipo de trabajo del proceso Acceso y Fortalecimiento a la Justicia (AJ), que el cargue de evidencias del primer cuatrimestre de riesgos de seguridad de Información se presentará de acuerdo con las recomendaciones de la OCI.

- Recomendación riesgo 3 - control 1: Ajustar Control.

Para esta recomendación, se informó por parte del equipo de trabajo del proceso Acceso y Fortalecimiento a la Justicia (AJ) - (CER), que dentro de las evidencias presentadas para el primer cuatrimestre de riesgos de seguridad de Información se entregara de acuerdo con las recomendaciones de la OCI.

En el ejercicio de la validación de este riesgo se presenta propuesta por parte del equipo de trabajo del proceso Acceso y Fortalecimiento a la Justicia (AJ), sobre ajustes referentes a el riesgo 3 - control 1:

Control Inicial:

Los profesionales especializados encargados del área Jurídica y Atención Integral del CER, revisan cuatrimestralmente la información de la solicitud de autorización de acceso a la documentación archivada, este profesional tendrá a su cargo las llaves del archivador de documentos, contará con un documento oficial y/o correo electrónico de personas autorizadas al acceso de la información archivada; 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.

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

Control Ajustado:

El 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

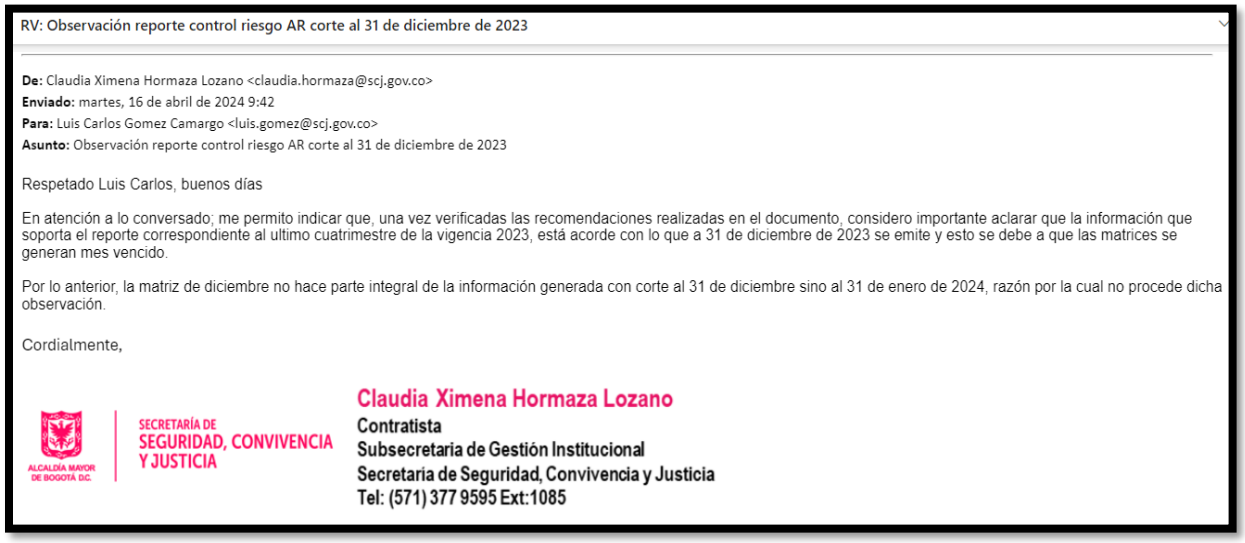
2.2.2. Proceso Atención y relación con el Ciudadano (AR).

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

Revisado el control No. 1 del riesgo No. 4 con los responsables de primera línea de defensa y el oficial de seguridad de la información, quedó claridad sobre la consistencia en su diseño y ejecución dentro de los parámetros de la guía de administración de riesgos de la SDSCJ.

Debido a que las evidencias de diciembre 2023 se generan mes vencido; la matriz de la información del mes en mención se realizó en el mes de enero de 2024 y se aportó como soporte de dicho mes es decir en el primer cuatrimestre de 2024. Por lo anterior, desde la OAP se hace la recomendación, que se analice la pertinencia de registrar esta desviación u observación en el control, y se pueda informar oportunamente por correo electrónico y/o documento oficial cuando la información no este completa por corresponder al mes vencido.

Al respecto de lo recomendado, el equipo de trabajo del proceso Atención y Relación al Ciudadano (AR), manifiesta que no procede y que se aclaró esta situación en reunión llevada a cabo con el ingeniero a cargo del reporte de los riesgos de la DTSI para lo cual se envió un correo, que respalda dicha aclaración sobre la información de la matriz del mes de diciembre 2023.



RV: Observación reporte control riesgo AR corte al 31 de diciembre de 2023

De: Claudia Ximena Hormaza Lozano <claudia.hormaza@scj.gov.co>
Enviado: martes, 16 de abril de 2024 9:42
Para: Luis Carlos Gomez Camargo <luis.gomez@scj.gov.co>
Asunto: Observación reporte control riesgo AR corte al 31 de diciembre de 2023

Respetado Luis Carlos, buenos días

En atención a lo conversado; me permito indicar que, una vez verificadas las recomendaciones realizadas en el documento, considero importante aclarar que la información que soporta el reporte correspondiente al ultimo cuatrimestre de la vigencia 2023, está acorde con lo que a 31 de diciembre de 2023 se emite y esto se debe a que las matrices se generan mes vencido.

Por lo anterior, la matriz de diciembre no hace parte integral de la información generada con corte al 31 de diciembre sino al 31 de enero de 2024, razón por la cual no procede dicha observación.

Cordialmente,

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

Claudia Ximena Hormaza Lozano
Contratista
Subsecretaria de Gestión Institucional
Secretaria de Seguridad, Convivencia y Justicia
Tel: (571) 377 9595 Ext:1085

Gráfica.3 Correo Electrónico como Evidencia.

2.2.3. Proceso Control Disciplinario (CID)

- ❖ Recomendación riesgo 7 - control 1: Revisión y ajustes de evidencias.

Para esta recomendación, se informó por parte del equipo de trabajo del proceso Control Disciplinario, que se ajustará las evidencias faltantes del tercer cuatrimestre 2023, al igual

se establece que para el seguimiento del primer cuatrimestre de riesgos de seguridad de Información vigencia 2024 se presentará de acuerdo con las recomendaciones de la OCI.

En el ejercicio de la validación de este riesgo se presenta propuesta por parte del equipo de trabajo del proceso Control Interno (CID), sobre ajustes referentes a el riesgo 7 - control 1

Control Actual:

El auxiliar administrativo de la oficina de Control Disciplinario Interno asignado, trimestralmente 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 enviara comunicación oficial y/o correo electrónico al Jefe de OCID 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.

De acuerdo con las revisiones y análisis del control se propone por parte del grupo estructurador del proceso Control Interno (CID), con apoyo de personal de la DTSI, el siguiente ajuste al control, así:

Control Ajustado:

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.

2.2.4. Proceso Fortalecimiento Institucional (FI).

- Recomendación riesgo 8 - control 1: Revisión y ajustes de evidencias.

Para esta recomendación, se informó por parte del equipo de trabajo del proceso Fortalecimiento Institucional (FI), que para el seguimiento del primer cuatrimestre de riesgos de seguridad de Información vigencia 2024 se presentara de acuerdo con las recomendaciones de la OCI.

2.2.5. Proceso Gestión Estratégica del Talento Humano (GH).

- Recomendación riesgo 9 - control 1: Ajustar Control.

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

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 a los 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 semestralmente.

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

Control Ajustado:

El 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.

- Recomendación riesgo 10 - control 1: Ajustar Control.

Para esta recomendación, se informó por parte del equipo de trabajo del proceso Gestión Estratégica del Talento Humano (GH), que se ajustará las evidencias del tercer cuatrimestre 2023 como se menciona en la observación, al igual se establece que para el seguimiento del primer cuatrimestre de riesgos de seguridad de Información vigencia 2024 se presentará de acuerdo con las recomendaciones de la OCI.

- Recomendación riesgo 11 - control 1: Ajustar Control.

En referencia al primer control del Riesgo 11 del GH, según la observación de la OCI, el activo en cuestión (Reporte de liquidación de nómina mensual) guarda una relación directa con los activos de información descritos en el riesgo 9, ya que están integrados en el sistema de información SIAP y pueden ser validados y controlados según los parámetros establecidos en el control designado para el Riesgo # 9 sobre control y acceso al sistema de información. Por consiguiente, se establece por parte grupo estructurador del proceso Gestión Estratégica del Talento Humano (GH) con el respaldo de la DTSI, la consolidación de estos activos (Riesgo 9 y Riesgo 11) para facilitar el seguimiento en el control asociado al Riesgo # 9.

2.2.6. Proceso de Gestión de Emergencias (GE).

- Recomendación riesgo 14 - control 2: Ajustar Control.

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

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

- ❖ Recomendación riesgo 14 - control 3: Ajustar Control.

Para esta recomendación, se informa por parte del equipo de trabajo del proceso de Gestión de Emergencias (GE), se realizó la validación del cargue de información y se borran los archivos que no corresponden a este control.

Gráfica.4 Ajuste Evidencia.

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

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

- ❖ Recomendación riesgo 18 – control 1: Ajustar Control.

En el ejercicio de la validación de riesgos se presenta propuesta por parte del equipo de trabajo del proceso Gestión de Seguridad y Convivencia (GS) sobre ajustes referentes a el riesgo 18 - control 1:

Control inicial:

El responsable de gestión de la información de Subsecretaría de seguridad y convivencia debe solicitar trimestralmente 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.

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

Control Ajustado:

El responsable de gestión de la información de 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.

18	Gestión de Seguridad y Convivencia.	1	Reducir el riesgo	Falta de control periodico sobre los derechos de acceso.	Pérdida o detrimento de información Demoras en los servicios prestados y ejecución de los procesos	El responsable de gestión de la información de Subsecretaría de seguridad y convivencia debe solicitar trimestralmente 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.	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.

Gráfica.5 Ajuste Control 18 - 1.

- Recomendación riesgo 18 – control 2: Ajustar Control.

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

Control inicial:

El responsable de gestión de la información de la Subsecretaría de seguridad y convivencia, verifica la construcción y actualización de una guía para el uso adecuado de la plataforma que incluya lineamientos para el registro y verificación de la información; una vez construida la guía se actualizará cuatrimestralmente, como evidencia se contara con el correo electrónico a los líderes de equipo para su debida implementación, en caso de no realizar la actualización de la guía se contara con comunicación formal al líder del proceso

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

Control Ajustado:

El 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.

18	Gestión de Seguridad y Convivencia.	2	Reducir el riesgo	Ausencia de guías para el adecuado uso de la plataforma.	Pérdida o detrimento de información Demoras en los servicios prestados y ejecución de los procesos	El responsable de gestión de la información de la Subsecretaría de seguridad y convivencia, verifica la construcción y actualización de una guía para el uso adecuado de la plataforma que incluya lineamientos para el registro y verificación de la información; una vez construida la guía se actualizará cuatrimestralmente, como evidencia se contara con el correo electrónico a los líderes de equipo para su debida implementación, en caso de no realizar la actualización de la guía se contara con comunicación formal al líder del proceso.	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.

Gráfica.6 – Ajuste Control 18 - 2.

- ❖ Riesgo 20 - control 1: Ajustar Control.

En el ejercicio de la validación de riesgos se presenta propuesta por parte del equipo de trabajo del proceso Gestión de Seguridad y Convivencia (GS) sobre ajustes referentes a el riesgo 20 - control 1.

Control Inicial:

El responsable de validar las Actas de los Consejos Locales de Seguridad en la plataforma dispuesta verifica mensualmente que los registros no contengan información sensible, en caso de evidenciar algún acta con este tipo de información registrarán en el formulario destinado para ello, la localidad en la que se presenta el hallazgo y notificará al dinamizador por correo electrónico para que el documento tenga el uso adecuado.

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

Control Ajustado:

El responsable de 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.

20	Gestión de Seguridad y Convivencia.	1	Reducir el riesgo	Acceso y uso inadecuado de la información	Pérdida o detrimento de información Perdida de confianza del ciudadano Demandas, litigios, derechos de petición o tutelas	El responsable de validar las Actas de los Consejos Locales de Seguridad en la plataforma dispuesta, verifica mensualmente que los registros no contengan información sensible, en caso de evidenciar algún acta con este tipo de información registrarán en el formulario destinado para ello, la localidad en la que se presenta el hallazgo y notificará al dinamizador por correo electrónico para que el documento tenga el uso adecuado.	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.

Gráfica.7 – Ajuste Control 20 - 1.

Así mismo, se establecieron las modificaciones sobre las variables Riesgo y Amenaza que complementan el ajuste enunciado para el control 20 y que responden a la realidad operativa de la gestión del activo, como se muestra a continuación:

20	Gestión de Seguridad y Convivencia.	**Actas de Concejos Locales de Seguridad.**	Información	Pérdida de la Disponibilidad	Gestion Inadecuada de la Información	
		Registros Survey 123 (Registros en el formulario)			Abuso de Derechos	

Gráfica.8 – Ajuste Control 20 -1.

Adicional, la Subsecretaría de Seguridad y la Dirección de Seguridad expusieron la intención de estudiar la posibilidad y realizar trámite para la eliminación de ese activo, dadas sus características de origen y el alcance que tiene la entidad en el manejo de este.

- ❖ Recomendación riesgo 21 - control 1: Ajustar Evidencias.

En el ejercicio de la validación de riesgos se presenta propuesta por parte del equipo de trabajo del proceso Gestión de Seguridad y Convivencia (GS) sobre ajustes referentes a el riesgo 21 - control 1.

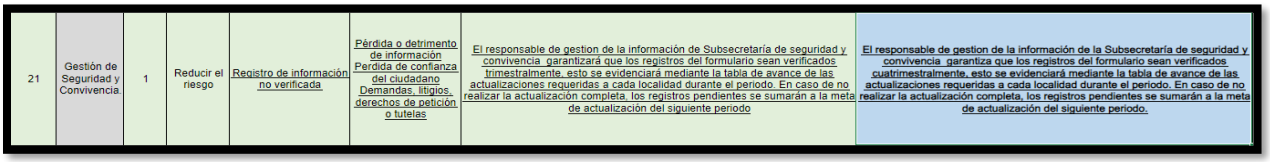
Control Inicial:

El responsable de gestión de la información de Subsecretaría de seguridad y convivencia garantizará que los registros del formulario sean verificados trimestralmente, 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:

Control Ajustado:

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.



21	Gestión de Seguridad y Convivencia.	1	Reducir el riesgo	Registro de información no verificada	Pérdida o detrimento de información Perdida de confianza del ciudadano Demandas, litigios, derechos de petición o tutelas	El responsable de gestion de la información de Subsecretaría de seguridad y convivencia garantizará que los registros del formulario sean verificados trimestralmente, 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	**El responsable de gestion 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.**

Gráfica.9 – Ajuste Control 21 - 1.

- Recomendación riesgo 22 - control 1: Ajustar Evidencias.

Para esta recomendación, se informó por parte del equipo de trabajo del proceso Gestión de Seguridad y Convivencia (GS), dentro de las evidencias presentadas se establece que para el cargue del primer cuatrimestre de riesgos de seguridad de Información se presentara de acuerdo con las recomendaciones de la OCI.

Control Inicial:

El responsable de gestión de la información de Subsecretaría de Seguridad y Convivencia verificará trimestralmente que al menos el 80% de los registros del formulario correspondan con las evidencias de las actividades realizadas durante el periodo mediante la tabla de verificación de correspondencia de registros. En caso de no cumplir con el porcentaje establecido se requerirá por correo electrónico a los responsables de las actividades para realizar la verificación respectiva.

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

Control Ajustado:

El responsable de gestión de la información de la Subsecretaría de Seguridad y Convivencia verifica de forma cuatrimestral que al menos el 80% de los registros del formulario correspondan con las evidencias de las actividades realizadas durante el periodo 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.

22	Gestión de Seguridad y Convivencia.	1	Reducir el riesgo	Dificultad para la verificación de los datos registrados	Pérdida o detrimento de información Perdida de confianza del ciudadano Demandas, litigios, derechos de petición o tutelas	El responsable de gestión de la información de Subsecretaría de Seguridad y Convivencia verificará trimestralmente que al menos el 80% de los registros del formulario correspondan con las evidencias de las actividades realizadas durante el periodo mediante la tabla de verificación de correspondencia de registros. En caso de no cumplir con el porcentaje establecido se requerirá por correo electrónico a los responsables de las actividades para realizar la verificación respectiva.	El responsable de gestión de la información de la Subsecretaría de Seguridad y Convivencia verifica de forma cuatrimestral que al menos el 80% de los registros del formulario correspondan con las evidencias de las actividades realizadas durante el periodo 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.

Gráfica.10 – Ajuste Control 22 - 1.

2.2.8. Proceso Gestión de Tecnología de Información (GT)

- Recomendación riesgo 23 - control 1: Ajustar Evidencias.

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

- Recomendación riesgo 23 - control 2: Ajustar Evidencias.

Control Inicial:

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

- Recomendación riesgo 24 – control 1: Ajustar Control.

Para esta recomendación, por parte del grupo de Infraestructura Tecnológica de la Dirección de Tecnologías y Sistemas de la Información, se realizará mesas de trabajo internas para atender las recomendaciones provistas de la OCI para el cierre del tercer cuatrimestre 2023 y se informa que para el primer cuatrimestre de riesgos de seguridad de Información 2024 se presentarán las evidencias del cargue del control de acuerdo con las recomendaciones de la OCI.

- Recomendación riesgo 24 – control 2: Ajustar Control.

Para esta recomendación, por parte del grupo de Infraestructura Tecnológica de la Dirección de Tecnologías y Sistemas de la Información, se propone eliminar el mencionado control tras evaluar que no es procedente mantenerlo y que no se podría cumplir, así:

Justificación para la Eliminación del Control 24-2

Contexto General:

El control 24-2 fue diseñado para fortalecer la disponibilidad y la continuidad operacional de la infraestructura tecnológica en la DTSI, mediante la reducción de la dependencia de un único proveedor de nube y la implementación de un plan de contingencia robusto. La finalidad era garantizar una gestión eficaz y segura de los servicios tecnológicos críticos.

Revisión por la OCI y Decisión del Equipo de Infraestructura de TI:

Una revisión reciente realizada por la Oficina de Control Interno (OCI) destacó la necesidad de generar evidencias más específicas y realizar validaciones adicionales del control. La OCI sugirió puntualizar cómo se garantiza la disponibilidad y reducir la dependencia de un único proveedor, en este caso Oracle Cloud. Sin embargo, esta recomendación excede la capacidad operativa y presupuestaria actual de la Entidad.

Problemas Identificados:

Capacidad Operativa y Presupuestal Limitada: La implementación de las recomendaciones de la OCI y los requisitos del control 24-2 requieren recursos, infraestructura y un presupuesto que actualmente no están disponibles. La dependencia de un único proveedor de nube es una consecuencia directa de las limitaciones presupuestarias y de infraestructura.

Desalineación con la Operación Actual: La recomendación de la OCI no alinea completamente con la comprensión y prácticas actuales del manejo de la infraestructura tecnológica y el respaldo de datos en la Entidad, lo que podría indicar un malentendido sobre las operaciones y capacidades actuales de la DTSI.

Decisión Unánime del Equipo de Infraestructura de TI: Dadas estas limitaciones y desafíos, el equipo de Infraestructura de TI, de manera unánime, ha decidido eliminar el control 24-2. Esta decisión está fundamentada en la inviabilidad de cumplir con las expectativas establecidas sin una revisión significativa de la estrategia de financiamiento y capacidad operativa.

Mitigación y Pasos Futuros: Para mitigar los posibles riesgos asociados con esta eliminación:

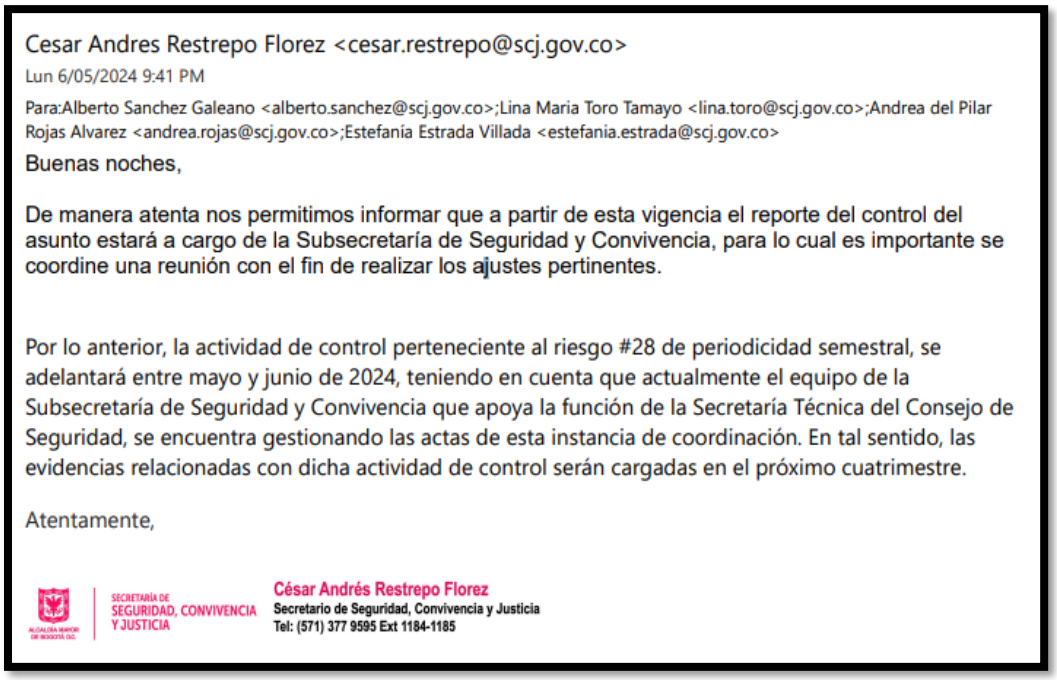
Proyección de Solicitud de Recursos: Se proyectará la solicitud de recursos adicionales en los próximos periodos fiscales para potencialmente expandir y diversificar la infraestructura tecnológica.

Revisión Estratégica: Se realizarán revisiones estratégicas de las operaciones tecnológicas para alinear las capacidades actuales y futuras con las necesidades operativas y de seguridad de la Entidad.

2.2.9. Oficina del Despacho (DES)

- Recomendación riesgo 28 - control 1: Ajustar Evidencias.

Para esta recomendación, se informó por parte del equipo de trabajo de la oficina del Despacho (DES), que a partir de esta vigencia el reporte del control del asunto estará a cargo de la Subsecretaría de Seguridad y Convivencia, por lo cual se hará los ajustes correspondientes y se entregarán las evidencias correspondientes, en los meses de mayo y junio 2024 así como las recomendaciones de la OCI sobre riesgos de seguridad de Información.



Cesar Andres Restrepo Florez <cesar.restrepo@scj.gov.co>
Lun 6/05/2024 9:41 PM
Para:Alberto Sanchez Galeano <alberto.sanchez@scj.gov.co>;Lina Maria Toro Tamayo <lina.toro@scj.gov.co>;Andrea del Pilar Rojas Alvarez <andrea.rojas@scj.gov.co>;Estefanía Estrada Villada <estefania.estrada@scj.gov.co>

Buenas noches,

De manera atenta nos permitimos informar que a partir de esta vigencia el reporte del control del asunto estará a cargo de la Subsecretaría de Seguridad y Convivencia, para lo cual es importante se coordine una reunión con el fin de realizar los ajustes pertinentes.

Por lo anterior, la actividad de control perteneciente al riesgo #28 de periodicidad semestral, se adelantará entre mayo y junio de 2024, teniendo en cuenta que actualmente el equipo de la Subsecretaría de Seguridad y Convivencia que apoya la función de la Secretaría Técnica del Consejo de Seguridad, se encuentra gestionando las actas de esta instancia de coordinación. En tal sentido, las evidencias relacionadas con dicha actividad de control serán cargadas en el próximo cuatrimestre.

Atentamente,

SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA
César Andrés Restrepo Florez
Secretario de Seguridad, Convivencia y Justicia
Tel: (571) 377 9595 Ext 1184-1185

Gráfica.11 – Correo Despacho.

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

# Riesgo	Proceso	Control	Comentarios
R11-C1	Gestión Estratégica del Talento Humano.	El equipo de nómina de la DGH, asigna y retira en caso de una novedad el permiso de acceso de usuarios autorizados de forma permanente a los repositorios asignados para el manejo de esta información, en caso de que los usuarios no cuenten con la autorización de acceso, no se permitirá la consulta a dichos expedientes, como evidencia se tendrán las comunicaciones de solicitud y retiro de acceso de usuarios. el cargue de evidencia se realizará Semestralmente	En referencia al primer control del Riesgo 11 del GH, según la observación de la OCI, el activo en cuestión (Reporte de liquidación de nómina mensual) guarda una relación directa con los activos de información descritos en el riesgo 9, ya que están integrados en el sistema de información SIAP y pueden ser validados y controlados según los parámetros establecidos en el control designado para el Riesgo # 9 sobre control y acceso al sistema de información. Por consiguiente, se establece por parte grupo estructurador del proceso Gestión Estratégica del Talento Humano (GH) con el respaldo de la DTSI, la consolidación de estos activos (Riesgo 9 y Riesgo 11) para facilitar el seguimiento en el control asociado al Riesgo # 9.

# Riesgo	Proceso	Control	Comentarios
R24-C2	Gestión de Tecnologías de la Información	El Líder o Coordinador de Infraestructura de TI de forma Anual o cada que se requiera es responsable de garantizar la disponibilidad de servicios internos de TI y reducir el riesgo de depender de un único proveedor de nube. Esto asegura la continuidad de las operaciones de la Entidad cuando hay cambios significativos en la infraestructura de TI o en la estrategia de proveedores de nube. Se verifica a través de desviaciones en el Plan de Contingencia de Servicios Tecnológicos y la Estrategia de Proveedores de Nube respaldados por la documentación correspondiente.	Por parte del grupo de Infraestructura Tecnológica de la Dirección de Tecnologías y Sistemas de la Información, se propone eliminar el mencionado control tras evaluar que no es procedente mantenerlo y que no se podría cumplir.
R28-C1	Gestión de Seguridad y Convivencia	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 a 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.	Por parte del equipo de trabajo de la oficina del despacho (DES), que a partir de esta vigencia el reporte del control del asunto estará a cargo de la Subsecretaría de Seguridad y Convivencia, por lo cual se hará los ajustes correspondientes y se entregaran las evidencias correspondientes, en los meses de mayo y junio 2024 así como los ajustes a las recomendaciones de la OCI sobre riesgos de seguridad de Información.

Tabla 1. Elaboración propia

Documentación Mesas de Trabajo:

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

https://scjgovcol.sharepoint.com/:f:/r/sites/DireccionTIC/Documentos%20compartidos/GobiernoTI/MIPG/Riesgos/Seguridad%20Informaci%C3%B3n/Informes/2024/Primer%20Cuatrimestre/Actas%20Mesa%20Trabajo?csf=1&web=1&e=CkhY9F

2.2. Matriz de Riesgos de Seguridad de la Información.

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

# Riesgo	Proceso/Dependencia	Riesgo	Control
R1-C1	Acceso y Fortalecimiento a la Justicia	Pérdida de la 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 Integridad	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 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

# Riesgo	Proceso/Dependencia	Riesgo	Control
R4-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.
R5-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.
R6-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 con el 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.
R7-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.
R8-C1	Fortalecimiento Institucional.	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.

# Riesgo	Proceso/Dependencia	Riesgo	Control
R9-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.
R10-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
R11-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.
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 Emergencias	Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad.	El responsable del proyecto NUSE123, de forma mensual verifica los informes de seguimiento a la operación entregados por la empresa ETB 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 el reporte que entrega la empresa ETB y/o el informe de interventoría, se realizaran las gestiones pertinentes mediante comunicado oficial y/o correo electrónico sobre la solicitud de información.

# Riesgo	Proceso/Dependencia	Riesgo	Control
R13-C2	Gestión de Emergencias	Ausencia de personal	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 las novedades.
R13-C3	Gestión de Emergencias	Gestión deficiente de contraseñas	El grupo de entrenamiento C-4, semestralmente, realiza capacitación y /o sensibilización a funcionarios y contratistas sobre el correcto uso de contraseñas de acuerdo con lo establecido en el manual de seguridad y privacidad de la información de la Entidad, como soporte de la evidencia se dejarán las listas de asistencia y documentos de apoyo de las capacitaciones, para los casos que personal no asista se procede con la reprogramación de una nueva sesión de capacitación.
R14-C1	Gestión de Emergencias	Respuesta inadecuada de mantenimiento del servicio.	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.
R15-C1	Gestión de Emergencias	Trabajo no supervisado del personal externo o de limpieza.	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 Data Center Bomberos) en caso de no contar con personal disponible de acompañamiento a la visita, no se autorizara el ingreso al personal externo y se reprogramara el mantenimiento. El cargue de las evidencias se hará de forma cuatrimestral.

# Riesgo	Proceso/Dependencia	Riesgo	Control
R15-C2	Gestión de Emergencias	Ausencia de acuerdos de nivel de servicio, o insuficiencia en los mismos.	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.
R16-C1	Gestión de Emergencias	Uso incorrecto de software y hardware.	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 Seguridad y Convivencia	Pérdida de la Integridad	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 a 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.
R18-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.

# Riesgo	Proceso/Dependencia	Riesgo	Control
R18-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.
R19-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.
R20-C1	Gestión de Seguridad y Convivencia	Pérdida de la Confidencialidad	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.
R21-C1	Gestión de Seguridad y Convivencia	Pérdida de la Integridad y Disponibilidad	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.
R22-C1	Gestión de Seguridad y Convivencia	Pérdida de la Integridad y Disponibilidad	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.

# Riesgo	Proceso/Dependencia	Riesgo	Control
R23-C1	Gestión de Tecnología de Información	Pérdida de la Integridad y Disponibilidad	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.
R23-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
R24-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.
R24-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.

# Riesgo	Proceso/Dependencia	Riesgo	Control
R25-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.
R26-C1	Evaluación al Sistema de Control Interno.	Pérdida de la Integridad	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 al 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.
R26-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 presentará el comunicado oficial enviado y las respuestas de los procesos y/o dependencias.
R27-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 solicitará a la DTSI se genere el reporte correspondiente por parte del administrador de la herramienta.

Tabla 2. Elaboración propia

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

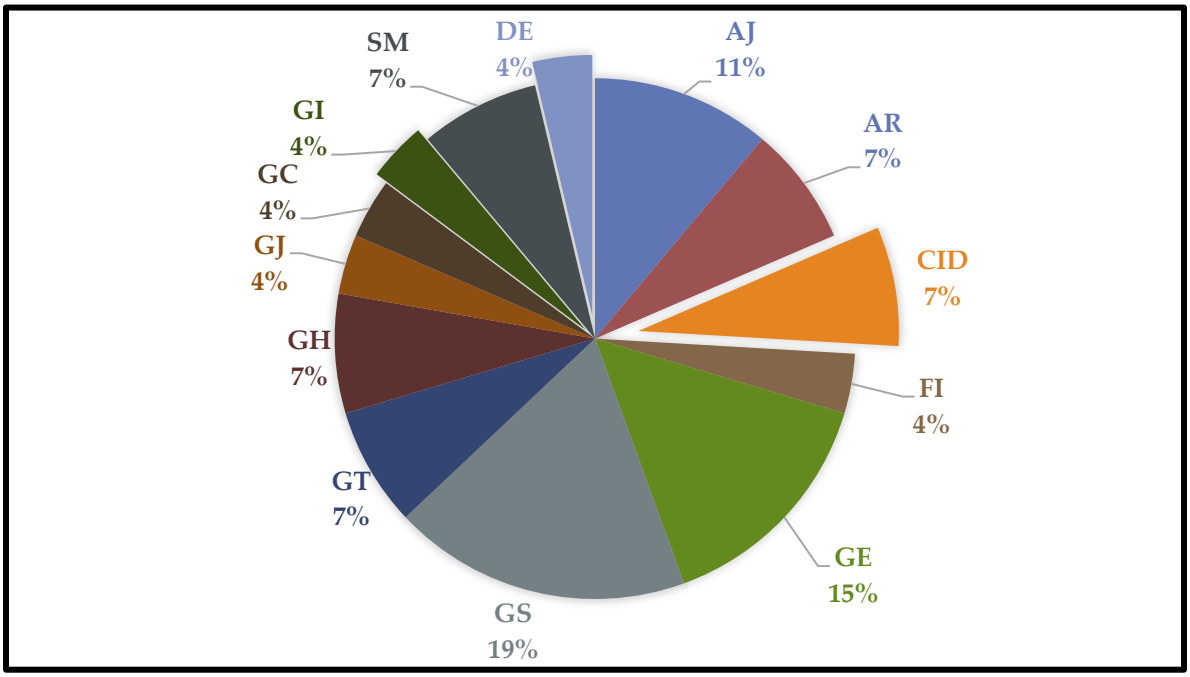
4. ANALISIS DE LA MATRIZ DE RIESGOS

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

PROCESO/DEPENDENCIA	SIGLA	RIESGOS
Acceso y Fortalecimiento a la Justicia	AJ	3
Atención y Relación con el Ciudadano.	AR	2
Control interno Disciplinario.	CID	2
Fortalecimiento Institucional.	FI	1
Gestión de Emergencias	GE	4
Gestión de Seguridad y Convivencia	GS	6
Gestión de Tecnología de Información	GT	2
Gestión Estratégica del Talento Humano.	GH	2
Gestión Jurídica	GJ	1
Gestión Contractual	GC	1
Gestión y Análisis de Información	GI	1
Evaluación al Sistema de Control Interno.	SM	2

Tabla 3. Elaboración propia

Porcentaje de Participación por Procesos/dependencias



Grafica 5. Elaboración propia

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%

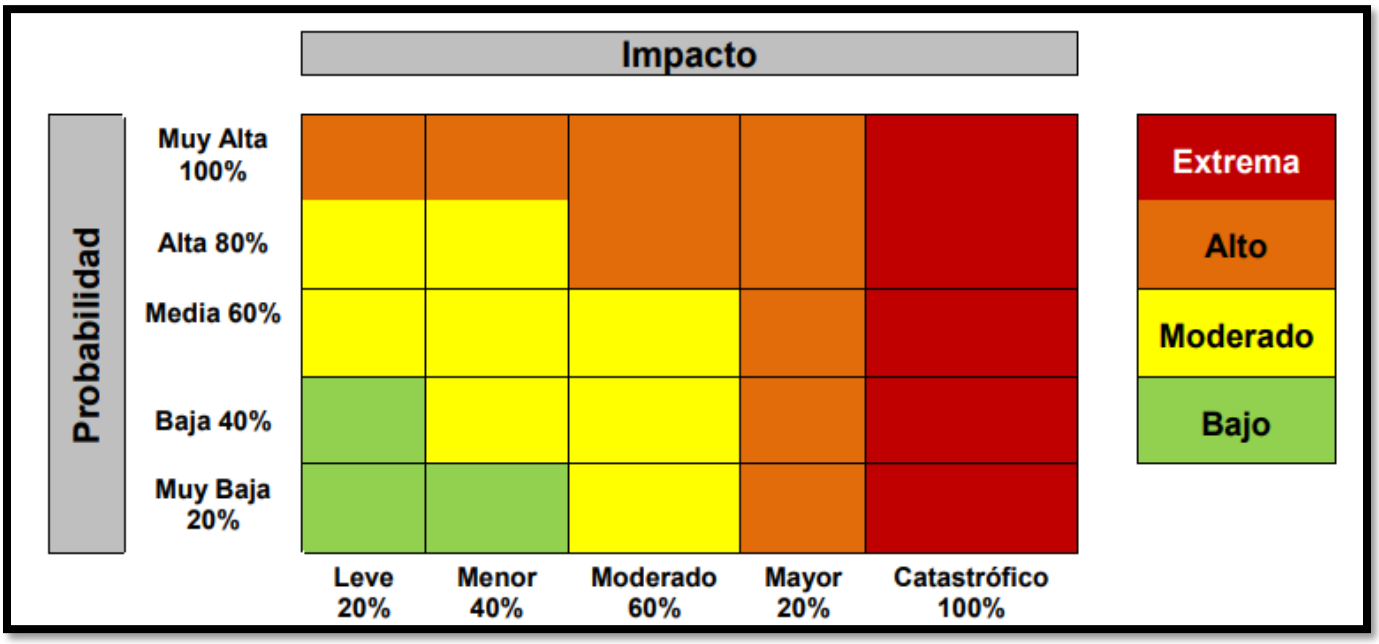
Grafica 6. Fuente: Política de Administración de Riesgos SDSCJ.

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 7. Fuente: Política de Administración de Riesgos SDSCJ.

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



Grafica 8. 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)			3		3
Atención y Relación con el Ciudadano (AR)			2		2
Control Interno Disciplinario (CID)			2		2
Fortalecimiento Institucional (FI)		1			1
Gestión de Emergencias (GE)			4		4
Gestión de Seguridad y Convivencia (GS)			6		6
Gestión de Tecnología de Información (GT)		2			2
Gestión Estratégica del Talento Humano (GH)			2		2
Gestión Jurídica (GJ)			1		1
Gestión Contractual (GC)			1		1
Gestión y Análisis de Información (GI)		1			1
Evaluación al Sistema de Control Interno (SM)			2		2
Total	**0**	**4**	**23**	**0**	**27**

Tabla 4. Elaboración propia

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.

La siguiente es la cantidad de riesgos y controles por proceso, aclarando que la cantidad de controles no está relacionada directamente con la materialización o no del riesgo. Los controles se han estructurado a consideración de cada proceso y sus recursos disponibles propendiendo evitar su posible materialización.

Proceso	N° Riesgos	N° Controles
Acceso y Fortalecimiento a la Justicia (AJ)	**3**	**3**
Atención y Relación con el Ciudadano (AR)	**2**	**2**
Control Interno Disciplinario (CID)	**2**	**2**
Fortalecimiento Institucional (FI)	**1**	**1**
Gestión de Emergencias (GE)	**4**	**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 Jurídica (GJ)	**1**	**1**
Gestión Contractual (GC)	**1**	**1**
Gestión y Análisis de Información de (GI)	**1**	**1**
Evaluación al Sistema de Control Interno (SM)	**2**	**3**
Total	**27**	**34**

Tabla 5. Elaboración propia

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)			3						3
Atención y Relación con el Ciudadano (AR)			2						2
Control Interno Disciplinario (CID)			2						2
Fortalecimiento Institucional (FI)		1							1
Gestión de Emergencias (GE)			4						4
Gestión de Seguridad y Convivencia (GS)			6						6
Gestión de Tecnología de Información (GT)		2							2
Gestión Estratégica del Talento Humano (GH)			2						2
Gestión Jurídica (GJ)			1						1
Gestión Contractual (GC)			1						1
Gestión y Análisis de Información de (GI)		1							1
Evaluación al Sistema de Control Interno (SM)			2						2
Total	**0**	**4**	**23**	**0**		**0**	**0**	**0**	**27**

Tabla 6. Elaboración propia

5. CARGUE EVIDENCIAS

Mediante memorando interno 3-2024-12538 de fecha 08/04/2024 - DTSI, se realizó solicitud de cargue de información para el primer 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 tercer cuatrimestre de 2023 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?csf=1&web=1&e=QNZB89

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**	**8**	100%
AR	Atención y Relación con el Ciudadano	**2**	**2**	**7**	100%
CID	Control Disciplinario	**2**	**2**	**4**	100%
FI	Fortalecimiento Institucional	**1**	**1**	**7**	100%
GC	Gestión Contractual	**1**	**1**	**1**	100%
GE	Gestión de Emergencias	**4**	**7**	**37**	100%
GH	Gestión Estratégica del Talento Humano	**2**	**2**	**6**	100%
GI	Gestión y Análisis de Información	**1**	**1**	**6**	100%
GJ	Gestión Jurídica	**1**	**1**	**1**	100%
GS	Gestión de Seguridad y Convivencia	**6**	**7**	**12**	100%
GT	Gestión de Tecnología de Información	**2**	**4**	**8**	100%
SM	Evaluación al Sistema de Control Interno	**2**	**3**	**4**	100%
	Total	**27**	**34**	**101**	**100%**

Tabla 6. Elaboración propia

Lo anterior significa que los lideres de procesos cumplieron con la entrega de las evidencias de ejecución de los controles a satisfacción basados los soportes suministrados, de esta forma se confirma la sobresaliente gestión realizada en términos generales por los procesos que hacen parte de la Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ relacionado a la Administración y Gestión de los Riesgos de Seguridad de la Información.

6. CONCLUSIONES

En resumen, al finalizar el primer cuatrimestre del año 2024, la Dirección de Tecnologías y Sistemas de la Información reafirma su compromiso y participación al revisar y dar seguimiento a la matriz de seguridad de información. Esto se hace en cumplimiento de la Política de Administración de Riesgos y los Lineamientos establecidos por la "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas - Versión 6 - noviembre de 2022" del Departamento Administrativo de la Función Pública (DAFP), con el respaldo continuo de los líderes operativos de cada proceso.

En la continuación del seguimiento durante el primer cuatrimestre del 2024 a los riesgos de seguridad de la información estructurados por los procesos enunciados, se puede concluir que la administración de los riesgos ha permitido la continuidad en la gestión, así como el logro de los objetivos definidos a los mismos, contribuyendo al fortalecimiento de la ejecución de actividades y el cumplimiento de los objetivos de la Entidad en materia de seguridad de la información.

Después de realizar mesas de trabajo con las áreas pertinentes, en respuesta al informe de seguimiento de la Oficina de Control Interno (OCI) con el radicado 3-2024-7270 “Informe de Seguimiento a Controles asociados a los Riesgos de Seguridad de la Información, Se ha

progresado considerablemente en la validación de las observaciones hechas, lo que ha facilitado una evaluación de los controles propuestos. Asimismo, se aprecia el compromiso y la colaboración de todas las áreas involucradas en estas acciones para implementar las mejoras sugeridas y mejorar 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 llevó a cabo la elaboración y envío de memorandos a todos los procesos de la Entidad, con el objetivo de la designación de los participantes en la actualización del registro de activos de información e índice de información clasificada y reservada para la vigencia 2024.

Es crucial destacar que el liderazgo en la implementación efectiva de la Política de Administración de Riesgos es liderado por la Dirección de Tecnologías y Sistemas de la Información para el caso de los Riesgos de Seguridad de la Información, con el apoyo de la Oficina Asesora de Planeación y el respaldo de la Oficina de Control Interno, ejercicio que es efectuado en conjunto con cada proceso por parte de los líderes operativos. Esto permite que la política se esté desarrollando y adoptando de manera adecuada durante el período actual en la Entidad.

Se resalta el compromiso evidenciado por los Líderes de Proceso y Líderes Operativos, junto con sus equipos, al desarrollar de manera efectiva los controles para los riesgos de seguridad de la información. Por ello, desde la Dirección de Tecnologías y Sistemas de la Información, deseamos expresar un merecido reconocimiento a todos los colaboradores que contribuyeron al cumplimiento de la meta del seguimiento y cargue de evidencias durante el primer cuatrimestre del año 2024.

La Dirección de Tecnologías y Sistemas de la Información, en su mejora continua, para el ejercicio sobre la gestión de Riesgos de seguridad para la vigencia 2024 de la información, reitera su responsabilidad y compromiso en el apoyo metodológico requerido ante las posibles modificaciones o ajustes de las caracterizaciones, procedimientos y documentación que respalde la gestión de cada proceso y que conlleven al potencial cambio de riesgos o controles actualmente identificados.