ALCALDÍA MAYOR DE BOGOTÁ
SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA
AL RESPONDER CITAR EL NR.
Nro. Rad: 3-2024-34703
Fecha: 21/10/2024 04:57:05 PM
Destino: 100-DESPACHO

MEMORANDO

Para: CESAR ANDRES RESTREPO FLOREZ
DESPACHO SECRETARIO DE SEGURIDAD

De: OFICINA DE CONTROL INTERNO

Asunto: INFORME DE SEGUIMIENTO A CONTROLES ASOCIADOS A RIESGOS DE SEGURIDAD DIGITAL CORRESPONDIENTE AL SEGUNDO CUATRIMESTRE DE 2024

Cordial saludo, Dr. Restrepo Florez:

En cumplimiento al Plan Anual de Auditoría 2024, la *Política de Administración de Riesgos de la Secretaría Distrital de Seguridad, Convivencia y Justicia (PO-FI-02 V2), y al Artículo 17 del Decreto 648 de 2017* respecto del rol *"Evaluación de la Gestión del Riesgo"*; esta oficina se permite comunicar el ***Informe de Seguimiento a controles asociados a los Riesgos de Seguridad de la Información***, correspondiente al segundo cuatrimestre de 2024.

Es preciso informar que, el documento será publicado en la sección de transparencia de la entidad a través del siguiente enlace:

https://scj.gov.co/es/transparencia/planeacion-presupuesto-ingresos/informes-control-interno:

- Informes de Ley y/o Seguimiento / Informes evaluación de riesgos y controles de seguridad digital / Informe de seguimiento a controles asociados a riesgos de seguridad digital - Segundo cuatrimestre de 2024.

Finalmente, esta oficina sugiere tener en cuenta las recomendaciones realizadas con el fin de identificar acciones que permitan aportar en el mejoramiento continuo y fortalecimiento institucional.

Cordialmente,

KAROL ANDREA PARRAGA HACHE
JEFE DE OFICINA CONTROL INTERNO

c.c.e.: IVAN HERSAYN PINILLA HERRERA-DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION
DIEGO MAURICIO USME GONZALEZ-DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION
Anexos: -1

Elaboró: ANDRES ORLANDO TORRES EUSSE
Revisó: ANDRES ORLANDO TORRES EUSSE-OFICINA DE CONTROL INTERNO -
Aprobó: KAROL ANDREA PARRAGA HACHE

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

Informe de Seguimiento a Controles asociados a los Riesgos de Seguridad de la Información

SEGUNDO CUATRIMESTRE 2024

Oficina de Control Interno

SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA

BOGOTÁ

1. OBJETIVO

Evaluar y realizar seguimiento a la implementación y diseño de los controles a través de los cuales se gestionan los Riesgos de Seguridad Digital de la Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ, de acuerdo con la ***PO-FI-02 Política de Administración de Riesgos. V2*** y la ***G-FI-04 Guía de Administración de Riesgos. V3,*** que forman parte del Sistema Integrado de Gestión - SIG.

1.1. OBJETIVOS ESPECIFICOS:

- Validar si los Riesgos de Seguridad de la información identificados y comunicados cumplen con lo establecido en la Política de Administración de Riesgos de la Entidad PO-FI-02- V2.
- Verificar si los veintiún (21) procesos de la SDSCJ cuentan con controles asociados a Seguridad de la información.
- Revisar la estructura, diseño y ejecución de los controles asociados a los Riesgos de Seguridad de la información vigentes.

2. ALCANCE

El alcance del presente seguimiento comprende el periodo entre el 01 de mayo y el 31 de agosto de 2024, frente al seguimiento y validación del diseño, implementación y ejecución de los controles asociados a los Riesgos de Seguridad Digital; en el marco de lo definido en la ***Matriz de Riesgos de Seguridad de la Información (F-FI-1385)*** de la Secretaría Distrital de Seguridad, Convivencia y Justicia.

Lo anterior, teniendo en cuenta que, el numeral 13. titulado *PUBLICACIÓN, SEGUIMIENTO Y EVALUACIÓN A LOS RIESGOS* de la citada Política, establece que, corresponde a la Primera Línea de Defensa realizar el cargue de soportes documentales de la implementación de los controles; y a la Segunda Línea de Defensa realizar cuatrimestralmente el seguimiento a la Matriz de Riesgos y remitir informe del resultado a la Oficina de Control Interno.

3. NORMATIVIDAD

- Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6, emitida por el DAFP.
- Guía de Administración del Riesgo de la SDSCJ (G-FI-04 V3)
- Política de Seguridad y Privacidad Información de la SDSCJ (PO-GT-1)
- Política de Administración de Riesgos de la SDSCJ (PO-FI-02 V2)
- Matriz de Riesgos de Seguridad de la Información de la Entidad (F-FI-1385)

4. SEGUIMIENTO

Para el periodo objeto de seguimiento y con base en los documentos de referencia, en primera instancia se observa que el 11 de septiembre de 2024, se realizó la actualización y publicación en la página web de la entidad de la ***Matriz de riesgos de seguridad de la Información 2024***, sobre la cual, esta oficina adelantó las siguientes validaciones:

4.1 APLICACIÓN DE LA POLÍTICA Y GUÍA DE ADMINISTRACIÓN DE RIESGOS DE LA ENTIDAD:

- **Etapa 1: Conocimiento y divulgación:**

En referencia a la etapa de conocimiento y divulgación, esta Oficina evidenció que:

✓ El 09 de septiembre de 2024, el proceso de *Fortalecimiento Institucional* divulgó a través del portal MIPG de la Entidad, la actualización de la **Política de Administración de Riesgos de la SDSCJ (PO-FI-02 V2)**, aprobada en Comité Institucional de Coordinación de Control Interno el 30 de julio del 2024.

Este documento adopta los lineamientos establecidos en la *Guía para la administración del riesgo y el diseño de controles en entidades públicas. V6*, emitida por el *Departamento Administrativo de la Función Pública*; y suministra las pautas para la Administración del Riesgo de la Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ.

✓ El 08 de agosto del presente año, a través de Memorando SIGA 3-2024-25594 con asunto *"CONTROLES ESTABLECIDOS PARA ATENUAR LOS RIESGOS ASOCIADOS A LA SEGURIDAD DE LA INFORMACIÓN"*, la Dirección de Tecnologías y Sistemas de la Información – en adelante DTSI – comunicó a los Directores y Líderes de las dependencias la fecha límite para realizar el cargue de las evidencias correspondientes a los controles establecidos, a fin de mitigar los riesgos asociados a seguridad de la información para el segundo cuatrimestre de la presente vigencia.

✓ El 22 de agosto del año en curso se observó que, la DTSI generó la pieza de comunicación ***¡Seguridad de la Información, una Responsabilidad de Todos!***, en la cual se dio a conocer que, de acuerdo con el *Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información*¸ y a fin de dar cumplimiento a la *Política de Administración de Riesgos*; la entidad se encontraba en el proceso de cargue de evidencias y seguimiento a los controles asociados a los riesgos de seguridad de la información, a saber:

Imagen N° 1. Pieza de Comunicación - Seguimiento a riesgos de seguridad de la información
Fuente: E-mail remitido por la DTSI el día 22 de agosto de 2024

- ✓ El 26 de agosto de 2024, la DTSI remitió correo electrónico a cada una de las dependencias informando que *"(…) en cumplimiento a lo establecido en la Política de Administración de Riesgos de la Secretaria Distrital de Seguridad, Convivencia y Justicia, y siguiendo lo establecido por el Departamento Administrativo de la Función Pública, se informa que el próximo 31 de agosto se culmina el segundo cuatrimestre para la vigencia 2024, lo que implica el cargue de evidencias para los controles establecidos para mitigar los riesgos de Seguridad de la información para los meses de mayo, junio, julio, agosto del proceso (…)"*

  Asimismo, la Dirección solicitó a los procesos realizar los ajustes correspondientes, con base en las recomendaciones emitidas por la Oficina de Control Interno mediante el ***Informe del Primer cuatrimestre de 2024 sobre riesgos de seguridad de la información***.

- Etapa 2: Identificación de los activos de seguridad de la información:

Para esta etapa, es preciso identificar los activos de información de los procesos que hacen parte de la Secretaría Distrital de Seguridad convivencia y Justicia, de acuerdo con lo establecido en la ***Guía de Gestión de Activos de Información (G-GD-01)***, los cuales deben ser clasificados y valorados.

En ese orden, y como resultado de la revisión hecha al *Registro de Activos de Información e Índice de Información Clasificada y Reservada (F-GD-1081*), se observó que, de conformidad con lo observado por esta Oficina en el *Informe del Primer cuatrimestre 2024 sobre riesgos de seguridad de la información*, la Dirección de Recursos Físicos y Gestión Documental en acompañamiento con la Dirección de Tecnologías y Sistemas de la Información, adelantaron mesas de trabajo para la identificación y actualización de los activos de información en la entidad con los siguientes procesos: *"Gestión de Emergencias, Gestión Tecnológica de Seguridad y Emergencias, Gestión de Comunicaciones Estratégicas, Direccionamiento Estratégico, Fortalecimiento Institucional, Gestión del Conocimiento y la Innovación Pública, Control Disciplinario; y Evaluación al Sistema De Control Interno"*.

Lo anterior contradice lo comunicado en el *Informe Segundo Cuatrimestre Riesgos de Seguridad de la Información – 2024* allegado por la DTSI, a saber: *"(…) 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 (…)"* (negrilla fuera de texto), toda vez que, como se evidencia en los soportes allegados por la Dirección en la carpeta "Activos de Información", dichas mesas solo fueron celebradas con los procesos mencionados anteriormente.

En virtud de lo expuesto, a la fecha se encuentran registrados los mismos 331 activos de la vigencia 2023; los cuales según su importancia y nivel de criticidad se clasificaron de la siguiente manera:

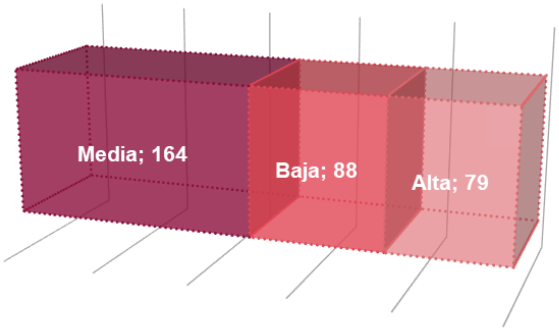

Gráfico N° 1. Activos de Información
Fuente: Informe Segundo Cuatrimestre Riesgos de Seguridad de la Información - 2024

De igual forma es pertinente aclarar que, como se cita en el Informe Segundo Cuatrimestre Riesgos de Seguridad de la Información – 2024 de la DTSI: *"(…) la actualización de los activos de información se tiene previsto de acuerdo con el Plan de tratamiento de riesgos de seguridad de la Información* ***para entrega durante la vigencia del tercer cuatrimestre de 2024"*** (negrilla fuera de texto), por lo cual, esta Oficina dará a conocer el resultado de dicha actualización en el seguimiento realizado para el periodo en mención.

Oportunidad de Mejora N° 01: Actualización del Formato F-GD-1081 Registro de Activos de Información e Indice de Información Clasificada y Reservada

De conformidad con los seguimientos realizados por la Oficina de Control Interno en el presente año y durante la vigencia 2023 se observa que, el ***Registro de Activos de Información e Índice de Información Clasificada y Reservada (F-GD-1081)*** no se ha actualizado desde el año 2022; evidenciando que, si bien durante el segundo cuatrimestre de 2024 se han adelantado mesas de trabajo con algunos procesos, a la fecha no se ha culminado el ejercicio de actualización de los activos de información de la Entidad.

Lo anterior, desconoce lo establecido en el numeral *7.2 ETAPAS DEL INVENTARIO DE ACTIVOS DE INFORMACIÓN* de la *Guía de Gestión de Activos de Información (G-GD-01)* que define: *"La identificación o actualización del inventario de activos de información, se realiza* ***anualmente*** (negrilla fuera de texto) *o cuando se requiera por cambios en la normatividad vigente, modificaciones en la estructura organizacional de la Secretaría Distrital de Seguridad, Convivencia*

y Justicia o en su mapa de procesos"; por lo que se recomienda a la DTSI dar cumplimiento y cierre del ejercicio de actualización durante el cuatrimestre en curso.

- Etapa 3: Pasos para la identificación y/o valoración de activos:

La Guía de Administración del Riesgo de la SDSCJ (G-FI-04) establece que, los Profesionales de Seguridad de la Información y Líderes de los procesos de la entidad, en conjunto con Gestión Recursos Físicos y Documental; deberán realizar la identificación y valoración de los activos de información, con base en: *"Información del proceso, Tipo de soporte, Tipo documental, Tabla de retención documental, Clasificación de la información, Criticidad del activo; e Infraestructura crítica cibernética"*

La Oficina de Control Interno realizó la validación de dichas variables contrastándolas con la estructura y los datos registrados en el *Registro de Activos de Información e Índice de Información Clasificada y Reservada (F-GD-1081)*, identificando lo siguiente:

- Información del proceso: El documento en la columna *"Tipo de activo"* incluye la tipificación establecida en la *Guía de Administración del Riesgo (G-FI-04)*, a saber: *"Información, Software, Servicio, Otros"*. Sin embargo, se recomienda que en el proceso de actualización del Registro, se incluyan activos que contengan la tipología *"Recurso Humano" y "Hardware"* también definidas en la Guía.

- Tipo de soporte: En las columnas *"Descripción del soporte"* y *"Formato"* del *F-GD-1081*, se evidencia el tipo de soporte, es decir, la definición del medio de conservación y/o soporte del activo, así como su respectivo formato.

- Tipo documental: De acuerdo con lo establecido en la Guía, esta información se encuentra registrada en el Formato, mediante las variables *"Nombre del activo (Registro o documento de archivo), Descripción del activo de información e idioma".*

- Tabla de retención documental: El Formato define el listado de series con sus correspondientes tipos documentales (subserie y descripción de la serie y/o subserie). No obstante, se evidencia el registro de treinta y cinco (35) activos de información clasificados como *"Sin establecer"* y un activo como *"N/A"*, por lo que se recomienda revisar los mismos en conjunto con el proceso de Gestión de Recursos físicos y Documental.

- Clasificación de la información: Se realiza la clasificación de la información de la Entidad en cada una de las siguientes columnas: *"¿Tiene datos personales?, Clasificación de la información, Custodio de la información, Estado de la información, Ubicación del activo de información, Publicada (link página web) y propietario del activo de información"*.

- Criticidad del activo: El Formato evalúa la criticidad de los activos de la Entidad, clasificando el grado de importancia de cada Activo de información de acuerdo con la Confidencialidad, Integridad y Disponibilidad (Alta, Media Baja).

- Infraestructura crítica cibernética: En la variable *"Infraestructura crítica cibernética"*, se identifica en el Registro la existencia de cuatro (4) activos de información con *Impacto Social* y un activo con *Impacto* Económico, todos con *Criticidad Alta*.

- ## Etapa 4: Identificación del riesgo

Como se ha mencionado, la Entidad adoptó los lineamientos establecidos en *la Guía de Administración del Riesgo (G-FI-04), la Política de Seguridad y Privacidad Información (PO-GT-1) y la Política de Administración de Riesgos (PO-FI-02 V2)*, como insumo para la elaboración de la *Matriz de riesgos de seguridad de la información.*

Es por ello por lo que, con base en la normatividad interna, la SDSCJ realizó la identificación y clasificación de los riesgos inherentes de seguridad de la información, así: *Pérdida de la confidencialidad, Pérdida de la integridad y Pérdida de la disponibilidad*.

Dicho ejercicio se llevó a cabo con base en la clasificación realizada para los 331 activos de información, de los cuales setenta y nueve (79) de ellos tuvieron ***Criticidad Alta*** y sirvieron como insumo para la identificación de los veintisiete (27) riesgos de la Matriz de riesgos de Seguridad de la Información, definidos por proceso así:

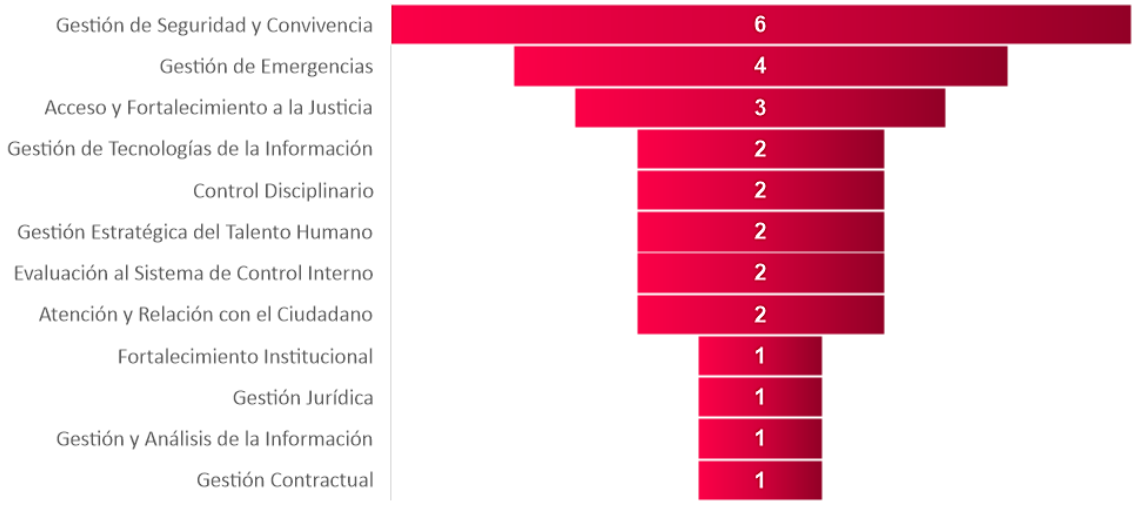

Gráfico N° 2. No. de Riesgos de seguridad de la información por Proceso
Fuente: Informe Segundo Cuatrimestre Riesgos de Seguridad de la Información - 2024

Es de precisar que, si bien cada riesgo asocia un grupo de activos específicos por proceso, y sobre ellos se analizan las posibles amenazas, vulnerabilidades y consecuencias que podrían causar su materialización; no se observa de manera detallada cual es la homologación de los setenta y nueve (79) activos con ***Criticidad Alta*** con los veintisiete (27) riesgos identificados en la Matriz; por lo que, esta Oficina reitera las recomendaciones hechas en Informes anteriores, respecto a la revisión y homologación de los datos de *Registro de Activos de Información e Índice de Información Clasificada y Reservada (F-GD-1081)* con lo identificado en la Matriz de riesgos de seguridad de la información.

Ahora bien, se reitera lo comunicado en el **Informe de Seguimiento a controles asociados a los Riesgos de Seguridad de la Información - Primer cuatrimestre de 2024**, a saber: *"(…) en el Formato F-GD-1081 se evidencia que del total de activos registrados en la hoja "LISTADO DE ACTIVOS – ICC" no existe ninguno clasificado como Hardware en la variable "Tipo de Activo"; lo que resulta contradictorio al revisar la agrupación realizada en la hoja "RIESGO INHERENTE", en donde se identifican cuatro (4) riesgos con este tipo de activo:(…)"*

RIESGO #	PROCESO	ACTIVO	TIPO DE ACTIVO
14	Gestión de Emergencias	Emerson Network Power Site Interface Card	Hardware
15	Gestión de Emergencias	Sistema de Videovigilancia Ciudadana	Hardware
16	Gestión de Emergencias	Sistema de Comunicaciones	Hardware
24	Gestión de Tecnologías de la Información	Infraestructura y Plataforma Tecnológica SDSCJ	Hardware

Tabla N° 1. Activos de Información
Fuente: Matriz de Riesgos de Seguridad de la Información de la Entidad

- ## Etapa 5: Valoración del riesgo

Como se indicó en la *Etapa 4: Identificación del riesgo*, la Secretaria cuenta con veintisiete (27) riesgos identificados en la Matriz de riesgos de Seguridad de la Información y clasificados por proceso, sobre los cuales se realizó la respectiva valoración del riesgo de acuerdo con lo establecido en el *numeral 9.6 de la Guía de Administración del Riesgo (G-FI-04) de la SDSCJ*, la cual apropia lo indicado en la *"Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas" versión 6 – 2022* del Departamento Administrativo de la Función Pública DAFP.

En virtud de lo anterior, esta Oficina identificó que, en el *Formato F-GD-1081*, por cada riesgo se realizó la valoración de la Probabilidad, Impacto y con base en ello se obtuvo el Riesgo Inherente, obteniendo una calificación de veintitrés (23) riesgos *Moderados* y cuatro (4) Altos, a saber:

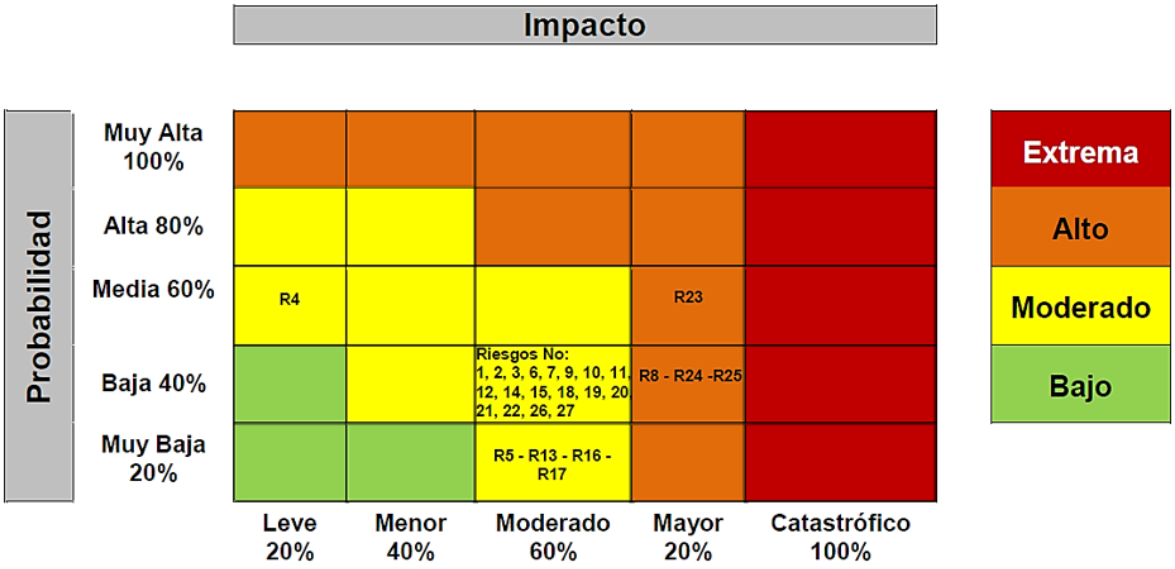

Imagen N° 2. Valoración del riesgo
Fuente: Elaboración Propia

De otra parte, al revisar el Mapa de procesos de la Entidad se evidenció que, no todos los procesos tienen Riesgos de Seguridad de la Información, a saber: *Direccionamiento Estratégico, Gestión de comunicaciones estratégicas, Gestión del conocimiento y la innovación pública, Gestión Documental, Gestión Financiera, Gestión de recursos físicos al servicio de la entidad, Gestión Integral a las personas privadas de la libertad – PPL, Administración de bienes muebles e inmuebles para el fortalecimiento de capacidades operativas, Gestión Tecnológica de Seguridad y Emergencias*.

Es de aclarar que, si bien esta situación fue puesta en conocimiento por la Oficina de Control Interno mediante el ***Informe del Tercer cuatrimestre de 2023 y Primer Cuatrimestre de 2024 sobre riesgos de seguridad de la información***, en soportes allegados por la DTSI se identificó la participación de los siguientes procesos en las mesas de trabajo realizadas para la identificación y actualización de activos de información de la Entidad: *"Gestión Tecnológica de Seguridad y Emergencias, Gestión de Comunicaciones Estratégicas, Direccionamiento Estratégico, Gestión del Conocimiento y la Innovación Pública".*

- ## Etapa 6: Creación de Controles

Esta Oficina observó que, la Matriz de Riesgos de Seguridad de la Información de la SDSCJ fue actualizada y publicada en la página web de la entidad el 11 de septiembre de 2024, y los cambios obedecen a ajustes en la descripción de algunos controles con base a lo observado por esta Oficina en el Informe de Seguimiento a controles asociados a los Riesgos de Seguridad de la Información - Primer cuatrimestre de 2024; por lo que, se conserva el total de veintisiete (27) riesgos identificados y treinta y cuatro (34) controles asociados, todos de *Tipo Preventivo*; clasificados por procesos, así:

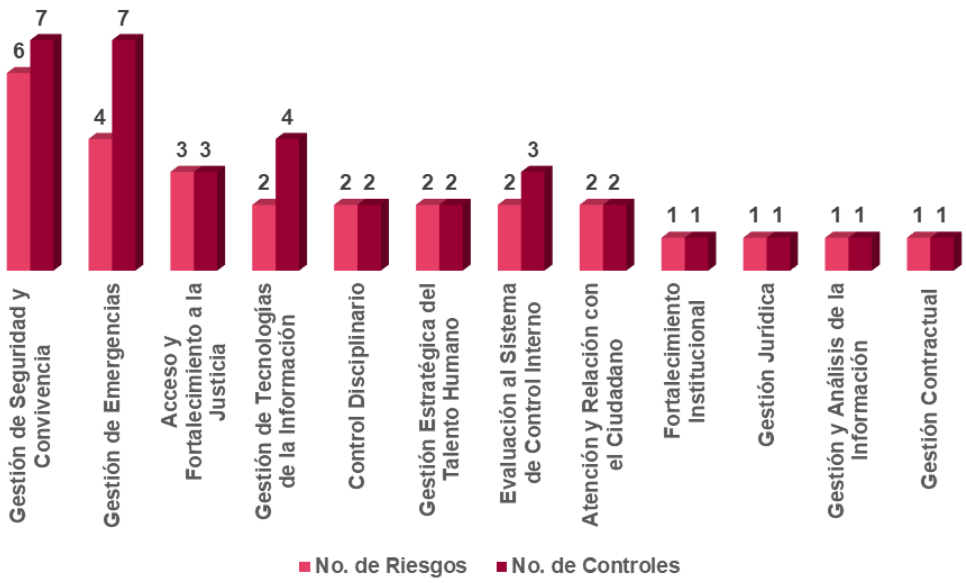

Gráfico N° 3– No. de Riesgos y Controles asociados, por Proceso
Fuente: Matriz de Riesgos de Seguridad de la Información

Ahora bien, en el *numeral 9.7.1 Estructura de Controles de la Guía de Administración del Riesgo (G-FI-04),* se establece que para que un control este adecuadamente diseñado y que su implementación sea efectiva, éste debe cumplir con los siguientes lineamientos:

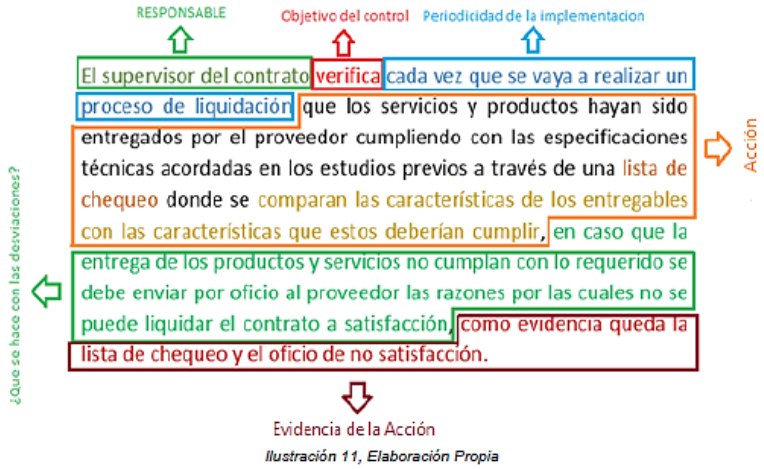

Imagen N° 3. Características de un control adecuadamente estructurado
Fuente: Guía de Administración del Riesgo (G-FI-04)

En ese orden, se evidenció a través de las respectivas actas de reunión que, en los meses de julio y agosto del presente año la DTSI celebró mesas de trabajo con cada uno de los procesos que a la fecha tienen riesgos de seguridad de la información, teniendo como objetivo contextualizar a los Lideres y/o enlaces de proceso sobre las recomendaciones dadas por la Oficina de Control Interno en el ***Informe de Seguimiento a controles asociados a los Riesgos de Seguridad de la Información - Primer cuatrimestre de 2024.***, las cuales fueron acogidas en la Matriz de Riesgos de Seguridad, registrando los siguientes ajustes:

- **Riesgo 2 - Control 1:** Revisión y ajuste de evidencias.
- **Riesgo 13 - Control 1:** Ajuste redacción del Control.
- **Riesgo 13 - Control 2:** Revisión y ajuste de evidencias.
- **Riesgo 14 - Control 1:** Revisión y ajuste de evidencias.
- **Riesgo 15 - Control 1:** Ajuste redacción del Control.
- **Riesgo 15 - Control 2:** Revisión y ajuste de evidencias.
- **Riesgo 16 - Control 1:** Revisión y ajuste de evidencias.
- **Riesgo 21 - Control 1:** Ajuste redacción del Control.
- **Riesgo 26 - Control 2:** Revisión y ajuste de evidencias.

Una vez validada la estructura de los treinta y cuatro (34) controles se observó que, si bien estos cumplen con los aspectos preceptuados en la ***Guía - G-FI-04***, es decir, se identifica: *Responsable, Objetivo del control, periodicidad, acción y evidencia de esta; y que se debe hacer en caso de presentarse desviaciones*; es importante que la 1LD y 2LD verifiquen en la descripción de los controles, si la acción establecida es coherente con la evidencia de la acción y el objetivo del control. De igual forma, y según lo previsto en el antedicho documento: *"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"* **(negrilla fuera de texto)**; se recomienda revisar los controles en donde la variable *desviación* no obedece a lo citado en la guía.

Lo anterior, teniendo en cuenta lo observado por esta Oficina en el *numeral 5.2EVALUACIÓN DE LA EJECUCIÓN DE LOS CONTROLES del presente Informe.*

- ## Etapa 7: Tratamiento del Riesgo Residual

Teniendo en cuenta lo establecido en la *Guía de Administración del Riesgo (G-FI-04)* de la Entidad: *"(…) Todos los riesgos deben contar con algún tratamiento residual independiente de la Zona de Riesgo (...)*, se identificó que, los veintisiete (27) riesgos de Seguridad de la Información se clasificaron con tipo de tratamiento *Reducir el Riesgo*, lo que permitió pasar de un Riesgo Inherente con calificación de veintitrés (23) riesgos *Moderados* y cuatro (4) *Altos*, a veintisiete (27) riesgos con calificación de *Riesgo Residual Bajo.*

- ## Etapa 8: Monitoreo, revisión y reporte

La Oficina de Control Interno realizó la validación al cumplimiento de los cinco (5) aspectos y/o lineamientos definidos en la Guía, bajo los cuales la Entidad asegura que la gestión realizada se orienta a la correcta ejecución de los controles asociados a los riesgos de seguridad de la información, observando que:

ASPECTO	SEGUIMIENTO OCI
1. El Mapa de riesgos de seguridad de la información, debe contener aquellas acciones de control definidas para el manejo del riesgo, buscando prevenir o reducir el riesgo detectado, teniendo en cuenta su viabilidad técnica y financiera. El monitoreo de las acciones de tratamiento debe realizarlo el responsable del proceso.	Como se expuso en el ítem ***Etapa 6: Creación de Controles*** del presente documento, una vez validada la estructura de los treinta y cuatro (34) controles se evidencia que, si bien estos cumplen con los aspectos definidos en la Guía, es decir, se identifica: *Responsable, Objetivo del control, periodicidad, acción y evidencia de esta, y que se debe hacer en caso de presentarse desviaciones*; es importante tener en cuenta lo observado por esta Oficina en el *numeral 5.2EVALUACIÓN DE LA EJECUCIÓN DE LOS CONTROLES del presente Informe.*
2. El responsable del proceso debe verificar que los controles establecidos en la matriz de riesgos operen de manera adecuada para mitigar los riesgos.	Con base en lo mencionado en la ***Etapa 1: Conocimiento y divulgación*** y la ***Etapa 6: Creación de Controles***, durante el mes de agosto del presente año, la DTSI como segunda Línea de defensa realizó asesorías y seguimiento tanto en la definición de los controles, como en el reporte y cargue de las evidencias que daban cuenta del cumplimiento de las acciones definidas en la descripción del control.

ASPECTO	SEGUIMIENTO OCI
3. El seguimiento de los riesgos identificados (incluyendo el tratamiento) se debe realizar de manera cuatrimestral por cada uno de los líderes de los procesos, quienes reportarán a la Dirección de Tecnologías y Sistemas de la Información quien consolidará y posteriormente enviará a la Oficina Asesora de Planeación para su publicación.	En el ***Informe Segundo Cuatrimestre Riesgos de Seguridad de la Información – 2024***, elaborado por la Dirección de Tecnologías y Sistemas de la Información, se evidenció que, a traves de memorando interno *3-2024-25594* la Dirección realizó solicitud a los procesos para el cargue de información del segundo cuatrimestre de la vigencia 2024. Por lo que, a traves del enlace compartido por la DTSI, esta Oficina validó las evidencias correspondientes de los controles asociados a los riesgos definidos en la Matriz, cuyas observaciones se registran en el *numeral 5.2EVALUACIÓN DE LA EJECUCIÓN DE LOS CONTROLES del presente Informe.*
4. Anualmente se debe realizar la valoración de los riesgos de seguridad de la información con el fin de verificar que el tratamiento fue efectivo y los niveles de riesgo disminuyeron.	En los meses de julio y agosto de 2024 la DTSI celebró mesas de trabajo con los procesos *"Acceso y Fortalecimiento a la Justicia, Gestión de Emergencias, Gestión de Seguridad y Convivencia, y Evaluación al Sistema de Control Interno"*; con el objetivo contextualizar a los Lideres y/o enlaces de proceso sobre las recomendaciones dadas por la Oficina de Control Interno en el ***Informe del Primer cuatrimestre sobre riesgos de seguridad de la información.*** Este ejercicio sirvió como base para que las partes realizaran la validación tanto de los riesgos identificados como de controles asociados, y con base en ello, realizaran los respectivos ajustes que aplicaran, como se evidencia en la ***Etapa 6: Creación de Controles.***
5. El responsable de realizar el seguimiento a los riesgos de seguridad de la Información debe reportar cuatrimestralmente a la mesa técnica de Seguridad Digital.	Durante el periodo objeto de análisis, fue reportado por el contratista responsable de seguridad de la información (Oficial de seguridad), el ***Informe Segundo Cuatrimestre Riesgos de Seguridad de la Información – 2024.*** Sin embargo, una vez revisado el Informe por parte de esta Oficina se evidenció que, no hay coherencia entre lo descrito en el *numeral 6. CARGUE EVIDENCIAS* y la *Tabla 7* del documento. Lo anterior toda vez que, la DTSI afirma que el Porcentaje (%) de riesgos cubiertos con base a las evidencias allegadas por la 1LD, fue del 100%; y la Oficina de Control Interno observó controles con falta de completitud de soportes que justificaran la ejecución de los mismos.

Tabla N° 2. Etapa 8: Monitoreo, revisión y reporte
Fuente: Elaboración propia. Guía de administración de riesgos G-FI-04

5. EVALUACIÓN A LA MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN – EVALUACIÓN DE CONTROLES ASOCIADOS A RIESGOS

A corte 31 de agosto de 2024, esta Oficina observó que, la **Matriz de Riesgos de Seguridad de la Información** cuenta con un total de veintisiete (27) riesgos y treinta y cuatro (34) controles asociados; de los cuales y de acuerdo con el Mapa de procesos vigente de la entidad, de los 21 procesos, únicamente 12 de estos tienen identificados riesgos y controles de seguridad.

5.1. EVALUACIÓN DISEÑO DE RIESGOS Y CONTROLES:

De los 27 riesgos de seguridad de la informacion a cargo de 12 de los 21 procesos de la entidad, esta Oficina realizó la evaluación de los riesgos y los controles asociados, de acuerdo con lo establecido en la ***Guía de Administración del Riesgo (G-FI-04),*** emitida por la SDSCJ, evidenciando que:

- Se da cumplimiento a lo definido en el aparte ***11.3 Etapa 4: Identificación del riesgo*** de la Guía, que establece: *"(…) se podrán identificar tres (3) riesgos inherentes de seguridad de la información: Pérdida de la confidencialidad, Pérdida de la integridad y Pérdida de la disponibilidad.* ***En cada riesgo se deben asociar el grupo de activos*** (negrilla fuera de texto)*, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.*

- Con base en lo establecido en el ***numeral 9.6 Valoración del riesgo de la Guía de Administración del Riesgo (G-FI-04)*** se evidenció que, en la valoración realizada a los veintisiete (27) riesgos identificados en la Matriz de seguridad de la Información, se determinó la probabilidad de ocurrencia junto con el impacto y/o consecuencia por la posible materialización de los riesgos en la Entidad.

- En la descripción y estructura de los treinta y cuatro (34) Controles, se evidenció que, si bien estos cumplen con lo definido en la Guía, es decir, se identificó: *Responsable, Objetivo del control, periodicidad, acción y evidencia de esta, y que se debe hacer en caso de presentarse desviaciones*; es importante tener en cuenta lo observado por esta Oficina en el numeral 5.2EVALUACIÓN DE LA EJECUCIÓN DE LOS CONTROLES del presente Informe.

5.2. EVALUACIÓN DE LA EJECUCIÓN DE LOS CONTROLES

Para el seguimiento y evaluación de la ejecución de los controles definidos en la **Matriz de Riesgos de Seguridad** de la SDSCJ, la Oficina de Control interno verificó la coherencia, suficiencia y completitud de los soportes allegados por la primera línea de defensa, y el monitoreo hecho por la segunda línea de defensa (DTSI); identificando*:*

Riesgo	Proceso	Control	Evidencia de la acción	Seguimiento OCI
1	Acceso y Fortalecimiento a la Justicia.	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.	▪ Matriz de reporte con la información de las metas establecidas en el Plan de Acceso a la Justicia.	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).** 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 idónea para la ejecución del control.
2	Acceso y Fortalecimiento a la Justicia.	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.	▪ Correo electrónico con la solicitud de verificación de los permisos de derecho de acceso a los diferentes enlaces que almacenan los reportes de la Dirección de Acceso a la Justicia.	De acuerdo con los soportes presentados por el proceso, se evidencia que el control se ejecutó.
3	Acceso y Fortalecimiento a la Justicia.	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	▪ Matriz *"Registro de acceso al archivo del Centro Especial de Reclusión - C.E.R"*, donde se identifica los datos de: *fecha, nombre del solicitante, asunto sobre el cual se realiza la consulta, Inclusión folios a expediente; y finalmente si la solicitud contó o no con la debida autorización.*	De acuerdo con los soportes presentados por el proceso, se evidencia que el control se ejecutó.

Riesgo	Proceso	Control	Evidencia de la acción	Seguimiento OCI
4	Atención y Relación con el Ciudadano.	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.	▪ Correos electrónicos que dan cuenta del seguimiento mensual realizado durante el segundo cuatrimestre por parte del proceso a la información recibida en el Sistema de Gestión documental SIGA. ▪ Matriz de trazabilidad de las PQRSD atendidas por el Proceso de *Atención y Relación con el Ciudadano*, para los meses de mayo, junio, julio y agosto de 2024.	De acuerdo con los soportes presentados por el proceso, se evidencia que el control se ejecutó.
5	Atención y Relación con el Ciudadano.	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.	▪ Correo electrónico que da cuenta de la solicitud y reporte de los usuarios activos en el sistema de información de Cobro Persuasivo COPE, tanto con perfil de abogado o de consulta. ▪ Base de datos con la relación de usuarios activos según el perfil, donde se especifica la fecha de creación de este, su estado y el rol.	De acuerdo con los soportes presentados por el proceso, se evidencia que el control se ejecutó.
6	Control Disciplinario.	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.	▪ Correos electrónicos en los cuales el Técnico administrativo de la OCDI solicita acceso a las bases de datos de la Oficina para los Profesionales que ingresan a laborar al proceso. Asimismo se observa en los soportes citados la autorización previa del Jefe OCDI para dar acceso a los usuarios.	De acuerdo con los soportes presentados por el proceso, se evidencia que el control se ejecutó.

Riesgo	Proceso	Control	Evidencia de la acción	Seguimiento OCI
7	Control Disciplinario.	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..	▪ Correo electrónico mediante el cual el Técnico administrativo de la OCDI informa que, de acuerdo al cumplimiento establecido en la **Política de Administración de Riesgos de la Secretaria Distrital de Seguridad, Convivencia y Justicia**, se realizó la verificación de los usuarios que tienen acceso a los expedientes virtuales y digitalizados de la Oficina de Control Disciplinario Interno; y asimismo solicita confirmación al Jefe OCDI para que los funcionarios puedan continuar con el acceso a los expedientes digitales. De conformidad con el correo, la Jefe OCDI confirma el acceso a las personas mencionadas en el mismo.	De acuerdo con los soportes presentados por el proceso, se evidencia que el control se ejecutó.
8	Fortalecimiento Institucional.	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.	▪ Correos electrónicos en los cuales el Profesional designado por parte de la Oficina Asesora de Planeación realiza monitoreo a la actualización de la información contenida en el botón de transparencia de la página web de la entidad. De igual forma, se comparte archivo con la relación y/o registro de las publicaciones realizadas durante el segundo cuatrimestre de la vigencia.	De acuerdo con los soportes presentados por el proceso, se evidencia que el control se ejecutó.
9	Gestión Estratégica del Talento Humano.	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.	▪ Correos electrónicos en los meses de mayo y junio de 2024, en los cuales el Profesional designado por parte del proceso realiza solicitud a la DTSI a través de la cuenta soporte.tecnico@scj.gov.co, para habilitar los permisos de acceso de los usuarios en el Sistema Integrado de Administración de Personal SIAP.	De acuerdo con los soportes presentados por el proceso, se evidencia que el control se ejecutó.

Riesgo	Proceso	Control	Evidencia de la acción	Seguimiento OCI
10	Gestión Estratégica del Talento Humano.	La Dirección de Gestión Humana define el acceso de los usuarios autorizados y el equipo de archivo de la DGH, controlará el acceso al repositorio de historias laborales para la consulta y manejo de esta documentación, en caso de que los usuarios no cuenten con la autorización de acceso, no se permitirá la consulta a dichos expedientes, como evidencia se tendrá la base de préstamos de historias laborales. el cargue de evidencia se realizará Semestralmente.	▪ Formato de *Consulta y préstamo documental* con el registro de préstamos de historias laborales sobre las cuales se dio acceso y autorización en el primer semestre de la presente vigencia.	De acuerdo con los soportes presentados por el proceso, se evidencia que el control se ejecutó.
11	Gestión Jurídica.	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.	▪ Formato Único de Inventario Documental – FUID de la DJC, en el cual se evidencia el registro de los expedientes y su control respecto a la completitud y correspondencia de archivos, relacionando: *nombre e identificación de la persona, año, folio y estado del expediente, así como la fecha de inicio y terminación del Contrato.*	De acuerdo con los soportes presentados por el proceso, se evidencia que el control se ejecutó.
12	Gestión Contractual.	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.	▪ Formato Único de Inventario Documental – FUID de la DJC, en el cual se evidencia el registro de los expedientes y su control respecto a la completitud y correspondencia de archivos, relacionando: *nombre e identificación de la persona, año, folio y estado del expediente, así como la fecha de inicio y terminación del Contrato.* ▪ *g*	De acuerdo con los soportes presentados por el proceso, se evidencia que el control se ejecutó.

Riesgo	Proceso	Control	Evidencia de la acción	Seguimiento OCI
13	Gestión de Emergencias.	El responsable del proyecto NUSE123, de forma mensual verifica los informes de seguimiento a la operación entregados por el operador tecnológico y los informes de interventoría del cumplimiento aprobados para los tramites de pagos correspondientes. como evidencia se entregan los informes de seguimiento a la operación, informe de interventoría y el informe de supervisión, 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.	▪ Informes de Gestión Operación NUSE 123 del Convenio Interadministrativo 561 Del 2014, para los meses de mayo y junio de 2024, pero no se evidencia los Informes correspondientes a julio y agosto. ▪ Informes de Supervisor de Contratos diferentes a OPS (F-GCT-1139. V.1), para los meses de mayo y junio de 2024, pero no se evidencia los Informes correspondientes a julio y agosto. ▪ No se evidencian los Informes de Interventoría. Lo anterior, pese a que el control define *(…) 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 (…)"*	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 idonea 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.
13	Gestión de Emergencias.	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 entregará 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.	▪ Matrices de Proyección de turnos para la operación del C4, correspondientes a los meses de mayo, junio, julio y agosto de 2024.	De acuerdo con los soportes presentados por el proceso, se evidencia que el control se ejecutó.

Riesgo	Proceso	Control	Evidencia de la acción	Seguimiento OCI
13	Gestión de Emergencias.	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.	▪ Matriz con la relación de las capacitaciones realizadas durante el segundo cuatrimestre de 2024, así como los soportes de ejecución de estas: *Listados de asistencia de personal capacitado y documentos de apoyo (presentaciones) de las capacitaciones.*	De acuerdo con los soportes presentados por el proceso, se evidencia que el control se ejecutó.
14	Gestión de Emergencias.	El grupo de seguimiento de infraestructura tecnológica del C-4, realizan la verificación de acciones preventivas y correctivas a UPS y Planta eléctrica programados en el contrato de mantenimiento establecido por parte de la Secretaría Distrital de Seguridad, convivencia y Justicia. Como evidencia se 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.	▪ 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 Electrica, 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.

Riesgo	Proceso	Control	Evidencia de la acción	Seguimiento OCI
15	Gestión de Emergencias.	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.	▪ Acta de Conciliación Técnica- Financiera para el mes de mayo de 2024, que tuvo como objeto *"Conciliación Técnica-financiera para la ejecución del Contrato Nro. SCJ 1816-2023".* ▪ *Acta Conciliación ANS Mayo 2024* ▪ Acta de Conciliación Técnica- Financiera para el mes de junio de 2024, que tuvo como objeto *"Conciliación Técnica-financiera para la ejecución del Contrato Nro. SCJ 1816-2023".* ▪ *Acta Conciliación ANS Junio 2024* Sin embargo, dentro de los soportes allegados no se identificaron las Actas de conciliación para los meses de julio y agosto de 2024.	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 cargara en las evidencias del corte del próximo cuatrimestre"* **(negrilla** y subrayado fueta de texto**)***;* esta Oficina observa que, no hay completitud de los soportes allegados por el proceso que den cuenta de la ejecución idonea 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.
15	Gestión de Emergencias.	El jefe del C4 supervisa a la empresa contratista del mantenimiento del sistema de video vigilancia y garantías extendidas del Centro de Computo. Estas actividades se registran en los informes de gestión de la empresa contratista, los cuales son recibidos y 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.	▪ Informes mensuales de la empresa Contratista para los meses de mayo, junio y julio de 2024, pero no se evidencia el Informe correspondiente al mes de agosto.	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.

Riesgo	Proceso	Control	Evidencia de la acción	Seguimiento OCI
16	Gestión de Emergencias.	El jefe del C4 delega a la empresa contratista el mantenimiento y operación del sistema de comunicaciones. Estas actividades se registran en informes de gestión de la empresa contratista recibidos de forma mensual evidenciando la operación del sistema de comunicaciones controlada por ANS, que en caso de estar por debajo de umbral se penaliza económicamente. las Evidencia corresponde al Informe mensual de la empresa contratista. El cargue de las evidencias se hará trimestralmente.	▪ Informes mensual de actividades servicios del Contrato 760 de 2024 de la empresa Contratista para los meses correspondientes al segundo cuatrimestre de 2024.	De acuerdo con los soportes presentados por el proceso, se evidencia que el control se ejecutó.
17	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 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.	▪ Correo electrónico dirigido al Subsecretario de Seguridad y Convivencia, reportando cual es la persona que cuenta con la autorización citada en la descripción del control, evidenciando en este el tipo de permiso con el que cuenta.	De acuerdo con los soportes presentados por el proceso, se evidencia que el control se ejecutó.
18	Gestión de Seguridad y Convivencia.	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.	▪ Correo electrónico con la solicitud del reporte de usuarios actuales en el aplicativo Progressus, con el fin de realizar la verificación asociada en la descripción del Control. ▪ Matriz en Excel donde se relaciona ID y usuario actual en el aplicativo Progressus, así como el respectivo rol que tiene dentro del Sistema.	De acuerdo con los soportes presentados por el proceso, se evidencia que el control se ejecutó.

Riesgo	Proceso	Control	Evidencia de la acción	Seguimiento OCI
18	Gestión de Seguridad y Convivencia.	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.	▪ Acta de reunión celebrada el 29 de agosto de 2024 por el líder operativo de la Subsecretaría de seguridad y convivencia, con el fin de evaluar la necesidad de actualizar la **G-GS-06 Guía para el registro y validación de actividades en Progressus.** Como resultado de la sesión se concluye que, la actualización del documento se debe realizar en el último cuatrimestre del año.	De acuerdo con los soportes presentados por el proceso, se evidencia que el control se ejecutó.
19	Gestión de Seguridad y Convivencia.	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.	▪ Acta de reunión celebrada el 26 de agosto de 2024, la cual tuvo como objetivo realizar seguimiento al cargue de documentación en el Sitio SharePoint correspondiente al segundo cuatrimestre 2024,con el fin de dar cumplimiento a criterios de custodia y confidencialidad de la información generada por la dependencia.	De acuerdo con los soportes presentados por el proceso, se evidencia que el control se ejecutó.
20	Gestión de Seguridad y Convivencia.	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.	▪ Correos electrónicos para los meses de mayo, junio, julio y agosto de 2024, donde se evidencia el control mensual de seguridad de la información realizado para las actas de Consejos Locales de Seguridad – CLS.	De acuerdo con los soportes presentados por el proceso, se evidencia que el control se ejecutó.

Riesgo	Proceso	Control	Evidencia de la acción	Seguimiento OCI
21	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.	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.
22	Gestión de Seguridad y Convivencia.	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.	▪ Correo electrónico en el cual el responsable de la Subsecretaría de Seguridad y Convivencia adjunta evidencia de la ejecución del Control 1 - Riesgo 22, en la cual se relacionan los registros por subsanar, que aún no están en Survey123. Asimismo, en el correo se tipifican las causas que dieron lugar a dichas inconsistencias.	De acuerdo con los soportes presentados por el proceso, se evidencia que el control se ejecutó.
23	Gestión de Tecnologías 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.	▪ Correo electrónico con la bitácora de actividades ejecutadas durante el periodo, donde se relacionan las pruebas de funcionalidad ejecutadas asociadas a los sistemas de información.	De acuerdo con los soportes presentados por el proceso, se evidencia que el control se ejecutó.

Riesgo	Proceso	Control	Evidencia de la acción	Seguimiento OCI
23	Gestión de Tecnologías 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	▪ Correo electrónico en el cual se informa que, en el marco de la actualización de la documentación de la arquitectura de los sistemas de información, se adelantó la actualización del manual de desarrollo seguro que tiene como objeto proporcionar un marco claro y consistente para el desarrollo de software seguro y de alta calidad. De igual forma se manifiesta que, estas consideraciones técnicas integran la implementación de los lineamientos y recomendaciones definidas en el **Manual de Seguridad y Privacidad de la Información MA-GT-1 V4** de la Secretaría Distrital de Seguridad, Justicia y Convivencia.	De acuerdo con los soportes presentados por el proceso, se evidencia que el control se ejecutó.
24	Gestión de Tecnologías 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.	▪ Documento Interno del Equipo de Infraestructura de la DTSI, en el cual se establece el ***Mecanismo seguro y estandarizado para la gestión segura de credenciales de administración en la infraestructura tecnológica.***	De acuerdo con los soportes presentados por el proceso, se evidencia que el control se ejecutó.
24	Gestión de Tecnologías 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.	▪ Documento PDF que contiene el reporte de rendimiento de la infraestructura de seguridad de la Secretaría Distrital de Seguridad, Convivencia y Justicia.	De acuerdo con los soportes presentados por el proceso, se evidencia que el control se ejecutó.

Riesgo	Proceso	Control	Evidencia de la acción	Seguimiento OCI
25	Gestión y Análisis de la Información.	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.	▪ Documentos en Excel para los meses de mayo, junio, julio y agosto de 2024, donde se relacionan las Consultas SQL realizadas para los periodos. Asimismo, se adjunta Hoja de vida del indicador: *"Cumplimiento en la Actualización de la Bodega de Datos"*; y se evidencia el reporte de este en el Portal MIPG.	De acuerdo con los soportes presentados por el proceso, se evidencia que el control se ejecutó.
26	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 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.	▪ Correo electrónico en el cual se evidencia la autorización de acceso de los usuarios a la información, previo requerimiento realizado por profesional de la DRFGD.	De acuerdo con los soportes presentados por el proceso, se evidencia que el control se ejecutó.

Riesgo	Proceso	Control	Evidencia de la acción	Seguimiento OCI
26	Evaluación al Sistema de Control Interno.	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.	▪ Memorando 3-2024-9876 emitido por la Jefe de la Oficina de Control Interno con asunto *"Socialización Versión 5 Procedimiento PD-SM-05 Planes de Mejoramiento Institucional - Contraloría de Bogotá y Presentación Profesionales de la Oficina de Control Interno responsables del seguimiento"*, en el cual se da a conocer la actualización realizada respecto a la actividad *Registrar el avance y/o gestión en la implementación de las acciones a través de la Plantilla de Seguimiento al PMI, con periodicidad trimestral".* De igual forma se cargan las respuestas de los procesos y/o dependencias, en respuesta al citado memorando.	De acuerdo con los soportes presentados por el proceso, se evidencia que el control se ejecutó.
27	Evaluación al Sistema de Control Interno.	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.	▪ Reporte de los Planes de Mejoramiento por procesos, y evidencia del cargue de los mismos en la TRD de la Oficina de Control Interno.	De acuerdo con los soportes presentados por el proceso, se evidencia que el control se ejecutó.

Complementario a lo anterior, pese a que para el *Informe Segundo Cuatrimestre Riesgos de Seguridad de la Información – 2024*, la DTSI manifestó el cumplimiento en el cargue de los soportes de la Primera Linea de Defensa, asociados a los controles de la Matriz de Riesgos de Seguridad de la Información; la Oficina de Control Interno observó que, dentro de las carpetas allegadas por la Segunda Línea de defensa, no se encontraba la completitud de los soportes de los siguientes controles: R1-C1, R13-C1, R14-C1, R15-C1, R15-C2, R21-C1; los cuales fueron calificados como incompletos frente a la evidencia de ejecución del control.

Cabe resaltar, que como se ha comunicado a traves de los diferentes Informes de Seguimiento a controles asociados a los Riesgos de Seguridad de la Información elaborados por esta Oficina, los controles asociados a los riesgos identificados para el proceso de *Gestión de Emergencias*, presentan reiteración en la incompletitud de los soportes allegados cuatrimestralmente, por lo que, se recomienda a la 1LD y 2LD, realizar una revisión y validación sobre la descripción del control y la evidencia de la acción relacionada.

6. CONCLUSIONES

- La Oficina de Control Interno realizó seguimiento a la ejecución de los controles a través de los cuales se gestionan los Riesgos de Seguridad Digital de la SDSCJ; observando que, como resultado del mismo, tres (3) riesgos presentaron debilidades en su diseño y un total de seis (6) controles fueron sujetos a observaciones en su ejecución asociados al soporte documental, a saber: R1-C1, R13-C1, R14-C1, R15-C1, R15-C2 y R21-C1.

- Se realizó validación del diseño de los controles, identificando que, si bien estos cumplen con la estructura definida en el ***numeral 9.7.1 Estructura de Controles de la Guía de Administración del Riesgo (G-FI-04)***; es importante que la 1LD y 2LD verifiquen en la descripción de los controles, si la acción establecida es coherente con la evidencia de la acción y el objetivo del control. De igual forma, y según lo previsto en el antedicho documento: *"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"* **(negrilla fuera de texto)**; se recomienda revisar los controles en donde la variable *desviación* no obedece a lo citado en la guía.

  Lo anterior, teniendo en cuenta lo observado por esta Oficina en el *numeral 5.2EVALUACIÓN DE LA EJECUCIÓN DE LOS CONTROLES del presente Informe.*

- Esta Oficina observó que, la **Matriz de Riesgos de Seguridad de la Información** cuenta con un total de veintisiete (27) riesgos y treinta y cuatro (34) controles asociados; de los cuales y de acuerdo con el Mapa de procesos vigente de la entidad, de los 21 procesos, únicamente 12 tienen identificados riesgos y controles de seguridad, a saber: *Gestión de Seguridad y Convivencia, Gestión de Emergencias, Acceso y Fortalecimiento a la Justicia, Gestión de Tecnologías de la Información, Control Disciplinario, Gestión Estratégica del Talento Humano, Evaluación al Sistema de Control Interno, Atención y Relación con el Ciudadano, Fortalecimiento Institucional, Gestión Jurídica, Gestión y Análisis de la Información, y Gestión Contractual*.

  Lo anterior pese a que, esta situación había sido informada por la Oficina de Control Interno mediante el ***Informe del Tercer cuatrimestre de 2023 y Primer Cuatrimestre de 2024 sobre riesgos de seguridad de la información***.

- De acuerdo con la información suministrada por la DTSI como 2LD, y con base en la evaluación realizada por la Oficina de Control Interno, no se evidenció la materialización de ningún riesgo de seguridad de la Información.

7. RECOMENDACIONES

- Evaluar el contenido y estructura del ***Informe Cuatrimestral de Riesgos de Seguridad de la Información – 2024*** generado por la DTSI, con el fin de que en el mismo se identifique de manera coherente y detallada el monitoreo realizado por la segunda línea de defensa a la ejecución adecuada de los controles; teniendo en cuenta la integridad, suficiencia, completitud y veracidad de las evidencias allegadas por la 1LD.

- Se sugiere a la segunda línea de defensa fortalecer el rol de asesoría y acompañamiento a los procesos de primera línea, a fin de generar alertas tempranas respecto a la gestión de los controles asociados a los riesgos, y la completitud, coherencia y suficiencia de los soportes allegados de los mismos; toda vez que, según lo establecido en el esquema de líneas de defensa de la ***Guía Rol de las Unidades u Oficinas de Control Interno, Auditoría Interna o quien haga sus veces***, es la segunda línea de defensa quien deberá contar con esquemas de seguimiento o autoevaluación permanente de la gestión, con el fin de orientar y generar alertas a las personas que hacen parte de la 1ª línea de defensa, así como a la Alta Dirección (Línea Estratégica).

Elaboró	Revisó
Andres Torres Eusse	Diego Alexander Urazan Franco
Contratista Oficina de Control Interno	Contratista Oficina de Control Interno

Aprobó

Karol Andrea Parraga Hache
Jefe Oficina de Control Interno