ALCALDÍA MAYOR DE BOGOTÁ
SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA
AL RESPONDER CITAR EL NR.
Nro. Rad: 3-2024-7270
Fecha: 21/02/2024 04:17:53 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 TERCER CUATRIMESTRE DE 2023

Cordial saludo, Respetado Doctor Restrepo:

De conformidad con los roles definidos para esta Oficina en cumplimiento del artículo 17 del Decreto 648 de 2017, así como del Plan Anual de Auditoria Vigencia 2023 y la Política de Administración de Riesgos PO-FI-02 Versión 1 y la Guía de administración de riesgos G-FI-04 Versión 1 de la Entidad, me permito remitir el informe de seguimiento a los controles asociados a riesgos de seguridad de la información correspondiente al tercer cuatrimestre de la vigencia 2023.

Como conclusión del ejercicio, informo que la entidad gestiona los riesgos y ha atendido las recomendaciones socializadas en anteriores informes de seguimiento por parte de esta Oficina, no obstante, se requiere intensificar las actividades propias correspondientes a la primera y segunda línea de defensa en el marco del Modelo Integrado de Planeación y Gestión - MIPG.

Finalmente, se sugiere que, debido a la evolución de la tecnología y por ende las amenazas digitales, para la gestión de los riesgos se implementen nuevos controles que permitan robustecer y/o blinden a la entidad respecto a la materialización de estos.

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
JOHN ALEXANDER HINCAPIE RUEDA-OFICINA ASESORA DE PLANEACION
Anexos: 1

Elaboró: DIEGO ALEXANDER URAZAN FRANCO-OFICINA DE CONTROL INTERNO
Revisó: DIEGO ALEXANDER URAZAN FRANCO-OFICINA DE CONTROL INTERNO |
Aprobó: KAROL ANDREA PARRAGA HACHE-OFICINA DE CONTROL INTERNO

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.

III Cuatrimestre de 2023

Oficina de Control Interno

SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA

BOGOTÁ

Tabla de contenido

1. OBJETIVO.

Evaluar, validar y realizar seguimiento de la adecuada implementación y diseño de los controles con los cuales se gestionan los riesgos de seguridad de la información con corte a 31 diciembre de 2023, basado en la versión 01 de la Política de Administración de Riesgos PO-FI-02 y la Guía de Administración de Riesgos G-FI-04 de la Secretaría Distrital de Seguridad, Convivencia y Justicia, documentos que fueron actualizados y generados en el mes de diciembre de la vigencia en mención.

2. ALCANCE.

Según lo planteado en el PAA (Plan Anual de Auditoría) del año 2023 y dando continuidad al seguimiento periódico que realiza la Oficina de Control Interno, esta actividad se enmarcó en el diseño y ejecución de los controles reportados por la Primera Línea de Defensa correspondiente al tercer cuatrimestre (septiembre a diciembre de 2023), dentro de la Matriz de Riesgos de Seguridad de la Información F-FI-1385 y los soportes o evidencias asociados.

3. METODOLOGÍA.

- ✓ Notificación del seguimiento a la Oficina Asesora de Planeación (en adelante OAP) por parte de la Oficina de Control Interno (en adelante OCI) al inicio de la vigencia.
- ✓ Requerimiento a la OAP de información consolidada de las evidencias y reportes realizados por la primera Línea de Defensa (procesos).
- ✓ Análisis de información suministrada por la Dirección de Tecnologías y Sistemas de la Información (en adelante DTSI) y consultada en el SharePoint donde se alojan las evidencias de ejecución de los controles, así como también la validación de documentación contenida en el Portal MIPG y la página web de la entidad.
- ✓ Inspección, análisis, validación y cotejo de evidencias.

4. RESULTADOS.

El seguimiento realizado y basados en los resultados obtenidos, de manera general nos permite informar que la entidad avanza respecto a la gestión de los riesgos de seguridad de la información, en anteriores ocasiones denominados de seguridad digital, alineándose con las mejores prácticas de la industria en dicha materia.

Para esto, la entidad realizó actualización de la política de administración de riesgos, la cual se complementó con el documento guía de administración de riesgos G-FI-04 Versión 1, donde puntualiza la metodología a aplicar para el tratamiento de los riesgos de seguridad de la información.

De acuerdo con lo mencionado, el siguiente es el detalle lo evidenciado donde se identificaron temas de mejora así:

4.1. Aplicación de la política y guía de administración de riesgos de la Entidad.

4.1.1. Etapa 1: Conocimiento y divulgación:

En referencia a la etapa de conocimiento y divulgación, la DTSI generó el día 7 de diciembre de 2023 una pieza comunicativa informando y socializando a toda la entidad el inicio del seguimiento a los controles de riesgos de seguridad de la información y compartiendo el acceso y/o consulta a la matriz relacionada.

Imagen N° 1: Fuente correo electrónico remitido por la DTSI el día 7 de diciembre de 2023

En relación a lo anterior, nos permitimos informar que la guía menciona ..” *Esta política debe ser de conocimiento general para los funcionarios directos e indirectos vinculados a la Secretaría Distrital de Seguridad, Convivencia y Justicia - SDSCJ, en el cual se especifican los lineamientos técnicos a seguir en la ejecución de la gestión del riesgo en la Entidad, con el fin de asegurar la integridad, disponibilidad, y confidencialidad de la información de sus procesos. ”.* por lo descrito y como oportunidad de mejora se informa que, para este caso de la pieza de comunicación generada y remitida como soporte, se hace referencia al inicio de un proceso de seguimiento, más no indica los lineamientos a seguir por parte de los funcionarios y contratistas respecto a la gestión del riesgo de seguridad de la información que permitan asegurar sus pilares; para tal fin, se sugiere que para esta fase de divulgación sean generadas indicaciones puntuales y asociadas a la gestión de los riesgos, sensibilizando de manera complementaria los documentos relacionados dentro del portal MIPG y la página web de la entidad.

4.1.2. Etapa 2: Identificación de los activos de seguridad de la información:

Como se mencionó en el informe de seguimiento del anterior corte (mayo a agosto de 2023), no se ha actualizado el inventario de activos de información, el cual contiene 331 ítems; por esto, nuevamente, se reitera y recomienda la actualización del inventario en mención, debido a que no se han generado activos de información para los nuevos procesos constituidos en la actualización del mapa de procesos institucional.

Por otra parte, como oportunidad de mejora se reporta que al validar el registro de activos de información publicado en la página web de la entidad en el vínculo: https://scj.gov.co/sites/default/files/instrumentos_gestion_informacion/RegistroActivosInformacion-IndiceInformacionClasificadayReservadada-SDSCJ_0_0.xlsx dentro de la sección https://scj.gov.co/es/transparencia/instrumentos-gestion-informacion-publica/registro-activos-informaci%C3%B3n/registro-2 no se está utilizando el formato oficial F-GD-1081 REGISTRO DE ACTIVOS DE INFORMACIÓN E INDICE DE INFORMACIÓN CLASIFICADA Y RESERVADA, el cual se encuentra vigente en el Portal MIPG, sino que el publicado es un archivo en Excel en formato no controlado.

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

La guía de administración de riesgos indica que, para la identificación de activos de información se deben tener en cuenta las siguientes variables que al validarlas contra la matriz REGISTRO DE ACTIVOS DE INFORMACIÓN contenida en el formato F-GD-1081 se obtiene lo siguiente:

Variable Guia administración de riesgo	Columna que homologa en el registro de activos de información	Adoptada en la entidad
Información del proceso	Id, tipo de proceso, proceso, código del procedimiento y código del formato	Si
Tipo de soporte	Tipo de activo, descripción del soporte y formato.	Si
Tipo documental	Nombre del activo (Registro o documento de archivo), Descripción del activo de información e idioma.	Si
Tabla de retención documental	Serie, subserie y Descripción de la serie y/o subserie (categoría de información).	Si
Clasificación de la información	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.	Si
Criticidad del activo	Importancia del Activo / Criticidad del Activo	Si
Infraestructura crítica cibernética	Impacto Social, Impacto Económico y Impacto Ambiental.	Si

Tabla N° 1 Elaboración propia. Fuente F-FI-1385_V Matriz de Riesgos de Seguridad de la Información.

Información del proceso:

En la guía se describe que los activos de la Entidad se clasifican en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada así: 1. Información 2. Software 3. Recurso Humano 4. Servicio 5. Hardware 6. Otros. Frente a esto y validando el documento fuente suministrado por la DTSI, se evidencia que en la columna tipo de activo se están utilizando las tipologías información, otros, servicios y software, por tanto, para el proceso de actualización que se vaya a ejecutar, se recomienda sean incluidos activos de información con las restantes tipologías descritas en la guía.

Infraestructura crítica cibernética

Para esta variable, se valida dentro del registro de activos de información, si la entidad ha identificado este tipo de infraestructura, identificando un ítem denominado NUSE (Número Único de Seguridad y emergencia

(Telefonía y CAD). No obstante, a lo mencionado y validando el soporte (acta) con al cual se determinó esta infraestructura crítica, no se tuvo en cuenta para la validación, lo descrito en la guía de administración del riesgos 12.2.1 Etapa 3: pasos para la identificación y/o valoración de activo - literal g Identificar si existen Infraestructuras Críticas Cibernéticas – ICC, la cual en su contenido literal define: ***Identificar y reportar a las instancias y autoridades respectivas en el Gobierno Nacional si la Entidad posee Infraestructura Critica Cibernética -ICC. Teniendo en cuenta que su impacto o afectación podría superar alguno de los siguientes criterios: Impacto social, Impacto económico e Impacto ambiental, conforme a la Guía para la Identificación de Infraestructura Crítica Cibernética (ICC) de Colombia, Primera Edición del Comando Conjunto Cibernético (CCOC), Comando General Fuerzas Militares de Colombia:***

IMPACTO SOCIAL (0,5%) de Población Nacional	IMPACTO ECONÓMICO PIB de un Día o 0,123% del PIB Anual	IMPACTO AMBIENTAL
250.000 personas	$464.619.736	3 años en recuperación

Imagen N° 2: Fuente guía de administración de riesgo pagina 54.

Lo anterior, indica que, para toda la plataforma tecnológica de la entidad, (nivel central y C4), se debió analizar y validar si algunos otros elementos, ejemplo sistema de video vigilancia o sistema de radio comunicaciones podrían quedar catalogados.

Con lo informado, se propone realizar un proceso de barrido para identificar, actualizar y confirmar activos de información asociados a la plataforma tecnológica de la entidad, los cuales puedan sean incluidos por su importancia como componentes de infraestructura critica cibernética, dejando las correspondientes evidencias de los ejercicios y análisis realizados.

4.1.4. Etapa 4: Identificación del riesgo:

Respecto a esta etapa, se indica que la entidad dentro de la matriz de riesgos de seguridad de la información ha adoptado lo descrito en la guía, consistente en la identificación y catalogación de los riesgos inherentes en perdida de confidencialidad, disponibilidad e integridad.

Si bien como se expresó, la entidad ha identificado los riesgos inherentes, dentro de la matriz de riesgos de seguridad de la información, se observa diferencia de datos, puesto que en el listado de activos identificados con criticidad ALTA - 79 de los 331 ítems (hoja LISTADO DE ACTIVOS - ICC) versus la hoja RIESGO INHERENTE el cual presenta 28 activos de información; cabe que resaltar que los activos fueron agrupados por temáticas, no obstante, se evidencia a manera de ejemplo el siguiente caso del proceso Acceso y Fortalecimiento a la Justicia:

Nombre activo (hoja LISTADO DE ACTIVOS - ICC)	**Importancia del Activo / Criticidad del Activo**	**Columna Riesgo Inherente – activos catalogados y agrupados** (hoja RIESGO INHERENTE)
Base de datos en Excel en donde se encuentra	Alto	• Documentación DAJ (Plan de Acción de Casas de Justicia, Actas del Comité de Coordinación Local de las Casas de Justicia, Acciones

Nombre activo (hoja LISTADO DE ACTIVOS - ICC)	Importancia del Activo / Criticidad del Activo	Columna Riesgo Inherente – activos catalogados y agrupados (hoja RIESGO INHERENTE)
toda la información de los ofensores y victimas vinculados al PDJJR. En las líneas de pos egreso y reintegro		Preventivo – Pedagógicas, Seguimiento a la Implementación del Traslado por Protección y Atención Psicológica a la Población Trasladada, Historias de Procesos de Mediación para la Solución de Conflictos). • Formularios (Formulario de forms registro atenciones virtuales Centro de Recepción e Información CRI, Formulario de forms registro jornadas unidades móviles para el acceso a la justicia, Formulario forms encuesta de satisfacción Dirección de Acceso a la Justicia). • Historia de PPL dentro del CER

Tabla N° 2 Elaboración propia. Fuente F-FI-1385_V Matriz de Riesgos de Seguridad de la Información.

Lo anterior indica una oportunidad de mejora respecto a la homologación de los datos de activos de información en la matriz de riesgos de seguridad de la información.

4.1.5 Etapa 5: Valoración del riesgo:

La entidad, continua con 28 riesgos identificados y segmentados por proceso así:

Proceso	Cantidad de Riesgos asociados
Gestión de Seguridad y Convivencia.	5
Gestión de Emergencias.	4
Gestión Estratégica del Talento Humano.	3
Acceso y Fortalecimiento a la Justicia.	3
Evaluación al Sistema de Control Interno.	2
Gestión de Tecnologías de la Información.	2
Control Disciplinario.	2
Atención y Relación con el Ciudadano.	2
Gestión y Análisis de la Información.	1
Fortalecimiento Institucional.	1
Sin Proceso	1
Gestión Contractual.	1
TOTAL	**28**

Tabla N° 3 Elaboración propia. Fuente F-FI-1385_V Matriz de Riesgos de Seguridad de la Información.

Como primera medida, desde la OCI informamos la catalogación de un activo de información que tiene asociado un riesgo de seguridad de la información, sin encontrarse asociado a ningún proceso. Dicho activo se titula: Actas del Consejo Distrital de Seguridad y Convivencia. Por lo anterior se presenta la oportunidad de mejora referente a la existencia de un activo de información que no pertenece a un proceso del actual

mapa de procesos de la entidad. Adicionalmente, se informa que no todos los procesos del actual mapa tienen riesgos de seguridad de la información, los cuales se relacionan: Gestión de comunicaciones estratégicas, Gestión del conocimiento y la innovación pública, Administración de bienes muebles e inmuebles para el fortalecimiento de capacidades operativas, Gestión Integral a las personas privadas de la libertad – PPL, Gestión de recursos físicos al servicio de la entidad y Gestión Documental y Gestión Financiera, situación que fue mencionada en el informe de seguimiento del periodo anterior.

De manera complementaria y de acuerdo con lo estipulado en la guía de administración de riesgos, se debe calcular la probabilidad impacto, para ser catalogado dentro del mapa de calor y así obtener el nivel de riesgo inherente. Para tal fin, en la hoja RIESGO INHERENTE de la Matriz de Riesgos de Seguridad de la Información para uno de los 28 riesgos, se calcula la probabilidad e impacto, obteniendo como resultado **24** riesgos moderados y **4** altos. Por lo mencionado, la entidad cumple con lo especificado.

4.1.6 Etapa 6: Creación de controles:

La guía de riesgos de la entidad establece que la estructura de controles debe cumplir con las siguientes variables: responsable, acción del control, soporte documental, periodicidad de la aplicación, objetivo y desviaciones entre el resultado esperado y obtenido así:

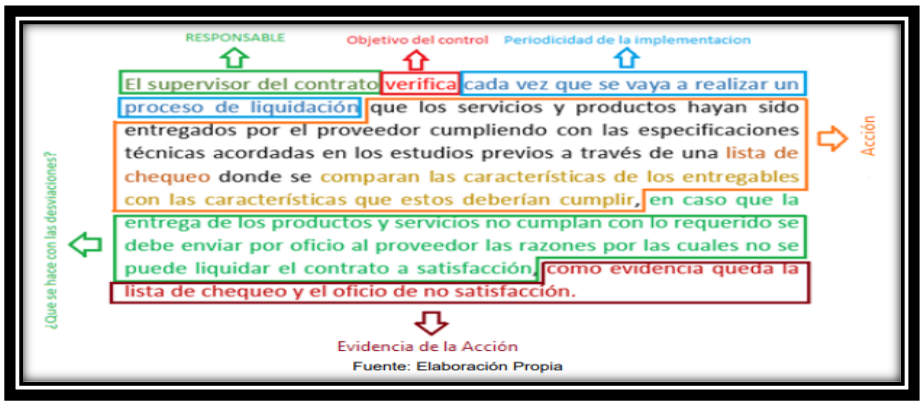

Imagen N° 3 Fuente Guía De Administración Del Riesgo G-FI-04 V1 pag 30.

Para este aspecto y al validar los 36 controles asociados a los riesgos de seguridad de la información, todos cumplen con las variables mencionadas. Se resalta la gestión realizada por la entidad, en el sentido que en el informe anterior se habían reportado controles sin claridad y que no cumplían la totalidad de las variables y al contrastarlos con la nueva versión de la matriz de riesgos de seguridad de la información, estos fueron ajustados.

Complementariamente, la guía describe que para los tipos de controles se definen 3:

a. Control Preventivo: (Entrada).
b. Control Detectivo: (Interrelaciones).
c. Controles Correctivos: (Salida).

En referencia al tipo, todos los controles asociados a los riesgos se encuentran catalogados como preventivos.

Y para la manera de cómo se ejecuta el control, se definieron dos tipologías: automáticos y manuales, no obstante, se presenta una oportunidad de mejora puesto que la matriz de riesgos de seguridad de la información no cuenta con estas dos tipologías determinadas para los 28 riesgos.

Cabe mencionar que, con la actualización de la matriz de riesgos de seguridad de la información, no hubo variación en la cifra de controles asociados a los riesgos así:

Proceso	Cantidad de controles identificados
Acceso y Fortalecimiento a la Justicia	3
Atención y Relación con el Ciudadano.	2
Control Disciplinario	2
Fortalecimiento Institucional.	1
Gestión de Emergencias	7
Gestión de Seguridad y Convivencia	6
Gestión de Tecnologías de la Información.	5
Gestión Estratégica del Talento Humano.	3
Gestión Contractual.	1
Gestión Jurídica.	1
Gestión y Análisis de la Información.	1
Evaluación al Sistema de Control Interno	3
Sin proceso	1
TOTAL	**36**

Tabla N° 4 Elaboración propia. Fuente Matriz de riesgos de seguridad de la información F-FI-1385 V1.

A pesar de que la cantidad de controles se mantuvo, en la actualización realizada a la matriz de seguridad de la información se presentaron los siguientes cambios:

a. El anterior proceso de gestión jurídica y contractual tenía dos controles asociados y al dividirse en dos procesos (gestión jurídica y gestión contractual en el nuevo mapa), de igual manera fueron redistribuidos uno para cada proceso.
b. En el informe anterior se presentó un control asociado al despacho, no obstante, para la presente versión de la matriz de riesgos de seguridad digital quedo bajo el nombre sin proceso.
c. Se actualizaron los nombres procesos de acuerdo con el nuevo mapa.

4.1.7. Etapa 7: Tratamiento del Riesgo Residual:

En este aspecto, la guía contempla que después de ejecutados los controles, se consideran 4 tipologías para el riesgo residual así:

- Aceptar.
- Reducir
- Evitar.
- Compartir.

En la entidad, los 28 riesgos de seguridad de la información quedaron catalogados en la tipología reducir.

4.1.8 Etapa 8: Monitoreo, revisión y reporte:

Esta etapa se compone de 5 puntos:

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.	La matriz de riesgos de seguridad de la información de la Secretaría cuenta con controles asociados a los riesgos determinados, todos dentro de un contexto de viabilidad respecto a su ejecución, por lo anterior se está cumpliendo este aspecto contemplado en la guía de administración de riesgos.
2. El responsable del proceso debe verificar que los controles establecidos en la matriz de riesgos operen de manera adecuada para mitigar los riesgos.	Se consulta a la DTSI, sobre el modo de cómo se ejecuta esta verificación por parte de los lideres o responsables del proceso , a lo cual fue respondido que *"Dando cumplimiento a lo requerido en el Ítem 2, durante el 2023 cuatrimestralmente, la Dirección de Tecnologías y Sistemas de la Información en el marco del proceso de verificación de los controles, con el fin de que operaran adecuadamente y de esta forma mitigar los riesgos, remitió memorandos y correos electrónicos a los líderes de los procesos de la Entidad con la verificación de los controles, informando detalladamente el grado de cumplimiento de estos de conformidad a lo establecido en la Política de Administración de Riesgos de la Entidad.* *Además de proporcionar información sobre los riesgos identificados y los controles implementados, se hace énfasis en la recolección de evidencias pertinentes que respalden la efectividad de dichos controles, particularmente en lo referente a la mitigación de riesgos de seguridad de la información* *Asimismo, se llevan a cabo mesas de trabajo periódicas con la participación de los responsables de los procesos y/o sus delegados. Estas mesas tienen como objetivo abordar y atender las observaciones y recomendaciones emitidas por la Oficina de Control Interno y efectuar la respectiva retroalimentación por parte de la Dirección de Tecnologías de la Información, en relación con los riesgos identificados y los controles implementados. Se establecen acciones para corregir deficiencias, fortalecer controles existentes o implementar cambios a los controles, según sea necesario, con el fin de mejorar continuamente la gestión de riesgos en la Entidad"*
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 del tercer cuatrimestre generado por la DTSI respecto a los riesgos de seguridad de la información, en el numeral 5 titulado cargue de evidencias, fue solicitado mediante memorando interno a todas las dependencias la ejecución de dicha actividad para el cuatrimestre; ante esto, se puso a disposición un repositorio en SharePoint del se informa que todos los controles contaron con la carga de soportes correspondiente, salvo uno del proceso Evaluación al Sistema de Control Interno que no se presentó para activar el control.

Aspecto	Seguimiento OCI
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.	Frente a este aspecto, se consulta a la DTSI, sobre la ejecución de esta valoración, a lo cual fue respondido que,*.." Durante el año 2022, se llevó a cabo la evaluación de los activos de información por parte de la DRFGD y la DTSI y se establecieron los riesgos y controles de seguridad correspondientes. Esto se logró mediante mesas de trabajo en las que participaron activamente los procesos y/o áreas responsables. Durante estas sesiones, se identificaron y analizaron los riesgos potenciales que podrían comprometer la seguridad de la información de la Entidad.* *En la vigencia 2023, se enfocó en la recopilación rigurosa de evidencias para respaldar la eficacia de los controles establecidos. Esto se llevó a cabo durante los tres (3) cuatrimestres de dicha vigencia, de acuerdo a lo definitivo en la Política de Administración de Riesgos. Cada trimestre, se realizó un seguimiento para verificar que los controles estuvieran operando de manera adecuada y efectiva en la mitigación de los riesgos identificados, tomando como referencia las recomendaciones establecidas por la Oficina de Control Interno.* *Es importante mencionar que, en lo referente a la vigencia 2023 en el primer cuatrimestre del 2024 se efectuará la valoración de los riesgos de seguridad de la información, con el fin de corroborar la efectividad de los mismos y la evaluación de los niveles de riesgo. Dicha actividad se efectuará con los procesos responsables por medio de trabajo donde evaluará la pertinencia de estos. "..* Por lo anterior, se enfatiza en la ejecución de esta valoración de manera prioritaria, puesto que en la vigencia 2023 no se ejecutó, lo cual incumple lo establecido en la guía de administración de riesgos numeral 11.7 Etapa 8: Monitoreo, revisión y reporte.
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 la vigencia 2023, en cada mesa técnica de seguridad digital, fue reportado por el contratista responsable de seguridad de la información (Oficial de seguridad), perteneciente a la DTSI, el seguimiento a los riesgos de seguridad de la información. La última mesa técnica fue realizada el día 7 de noviembre de 2023; por lo anterior se está dando cumplimiento a lo establecido en la guía de administración de riesgos.

Tabla N° 5 Elaboración propia. Guía de administración de riesgos G-FI-04 V.1

4.2. Matriz de riesgos de seguridad de la información – Evaluación de Controles asociados a Riesgos:

Como se ha informado a lo largo del presente informe de seguimiento, la matriz de riesgos de seguridad de la información F-FI-1385 V1 de la Entidad se compone de 28 riesgos con 36 controles asociados, para tal fin, y respecto a cada uno de estos, se procedió a evaluar los controles obteniendo los siguientes resultados:

RIESGO #	PROCESO	CONTROL #	CONTROL	Seguimiento OCI Tercer cuatrimestre 2023
1	Acceso y Fortalecimiento a la Justicia.	1	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.	Se evidenció un soporte el cual contiene correos electrónicos donde la contratista responsable solicita el reporte del plan de acceso a la justicia en el mes de diciembre de 2023 y enero de 2024. En el informe del anterior seguimiento fue informado que: , ***no se están adicionado soportes de entregas de información por parte de los responsables a la Dirección, ni tampoco se evidencian soportes donde se refleje que la DAJ ha solicitado o recordado la entrega oportuna de la información; una vez expresado lo anterior, no es posible determinar el cumplimiento total del control.*** Por lo anterior, se reitera la oportunidad de mejora y la recomendación de generar soportes que apunten a todos los activos de información catalogados, acompañados del respectivo monitoreo por parte de la segunda línea de defensa.
2	Acceso y Fortalecimiento a la Justicia.	1	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.	Se evidenció un soporte de correo electrónico emitido en el mes de diciembre de 2023, donde un profesional de la Dirección informa a los responsables de los formularios el ajuste de los permisos a cada uno de estos, derivado de los retiros que se han suscitado, por tanto, el control se encuentra operando correctamente. De acuerdo a lo mencionado y comparando con los anteriores periodos de seguimiento, se recomienda que la primera línea de defensa genere soportes adicionales o complementarios que reflejen el monitoreo o revisión en los formularios en mención, donde quede aprobado el personal que efectivamente corresponda y adicionalmente, el soporte de los informes remitidos al jefe de área en caso de encontrar diferencias.

3	Acceso y Fortalecimiento a la Justicia.	1	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.	La dependencia responsable remite evidencias asociadas al cumplimiento del control tal como se estipuló, informando para el tercer trimestre que el personal autorizado es el mismo de los periodos anteriores. En referencia al control y como parte de la dinámica de riesgos y controles, se recomienda que la segunda línea de defensa realice monitoreo de la ejecución del control en campo, para validar así su efectividad y cumplimiento, de lo contrario generar nuevas acciones que mitiguen los riesgos de seguridad de la información que pueda estarse presentando.
4	Atención y Relación con el Ciudadano.	1	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.	Se evidencian soportes asociados al cumplimiento del control en el tercer cuatrimestre de 2023 derivado de la verificación realizada. En referencia al tema de la matriz de trazabilidad descrita en el control, se observan las correspondientes a los meses de agosto, septiembre, octubre y noviembre, quedando pendiente la matriz de diciembre, por tanto, se recomienda que, para los reportes periódicos de evidencias del control posteriores, se complemente la información por parte de la primera línea de defensa.
5	Atención y Relación con el Ciudadano.	1	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.	Se evidencian soportes de correos electrónicos que dan cumplimiento del control establecido asociado al manejo de roles del sistema de información COPE.
6	Control Disciplinario.	1	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.	La dependencia responsable remite soporte donde menciona que no se presentaron autorizaciones de acceso a las bases de datos; por lo anterior, el control se encuentra operando correctamente.

7	Control Disciplinario.	1	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.	Se evidencia ejecución de control en el mes de diciembre de 2023, donde se ratifican los usuarios que tienen acceso a la información. Como oportunidad de mejora se menciona y recomienda a la primera línea de defensa remitir los soportes de todo el periodo, puesto que el control está programado trimestralmente y los soportes se remiten a la segunda línea cuatrimestralmente.
8	Fortalecimiento Institucional.	1	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,	Después de analizados los soportes asociados a la ejecución del control, informamos que se cuenta con la matriz de cumplimiento del índice de transparencia y acceso a la información. Una vez validada aleatoriamente la mencionada matriz, se evidencia que para el tema de rendición de cuentas a la ciudadanía, se reporta en el seguimiento con cumplimiento, no obstante al verificar el vínculo https://scj.gov.co/es/transparencia/planeacion-presupuesto-ingresos/informe-rendicion-ciudadania, no se observa la pestaña de la vigencia 2023; también, dentro del monitoreo no se observa algún tipo de comentario o nota por parte de la primera o segunda línea de defensa, razón que nos permite sugerir sobre ahondar los procesos de seguimiento, para así garantizar que las publicaciones en página web se cumplan para cada vigencia consistentemente.
9	Gestión Estratégica del Talento Humano.	1	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.	Se valida como evidencia un correo electrónico remitido por Talento Humano y contestado por DTSI en referencia a un retiro y asignación de permisos en el sistema de información SIAP. Por lo expuesto, el control está operando tal como está establecido. No obstante, a lo anterior, y debido a la existencia de controles con características similares asociadas a otros procesos, se recomienda evaluar la periodicidad establecida y de igual manera validar en el sentido que apunta a los accesos a repositorios de información y no al sistema de información de nómina. De igual manera y por el tema de la materialización de riesgo en la vigencia 2023 dentro del proceso de gestión estratégica del talento humano, se propone la creación de nuevos controles asociados al manejo de información en el sistema de información SIAP.

10	Gestión Estratégica del Talento Humano.	1	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	Se observan soportes asociados al control generados mensualmente desde julio a diciembre de 2023, donde se presentan los formatos con los registros de préstamos documentales; si bien el control se encuentra operando, se menciona y sugiere un monitoreo por las dos primeras líneas de defensa que apunte al completo diligenciamiento de la planilla contemplada en el control, puesto que en los meses de noviembre y diciembre se presentan campos de firmas sin diligenciar.
11	Gestión Estratégica del Talento Humano.	1	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	Para este control y de acuerdo con la revisión realizada de los soportes entregados por parte de la dependencia responsable, se sugiere este sea validado puesto que tiene similar redacción al control R09-C1, ya que incluso se está entregando el mismo soporte del mencionado control, el cual consiste en la remisión de un correo electrónico a la DTSI con las solicitudes de acceso y retiro de usuarios en el sistema de información SIAP.
12	Gestión Jurídica.	1	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.	Se evidencia soporte con el formato FUID de la vigencia 2023 asociado a la dependencia responsable, actualizado a diciembre de 2023, por lo anterior se está cumpliendo con el control de acuerdo con lo establecido.
13	Gestión Contractual.	1	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.	Se evidencia soporte con el formato FUID de la vigencia 2023, actualizado a diciembre de 2023, por lo anterior se está cumpliendo con el control de acuerdo con lo establecido.
14	Gestión de Emergencias.	1	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.	Frente a este control, la dependencia responsable remite los informes de gestión, interventoría y supervisión que se generan mensualmente (septiembre a diciembre de 2023). Por ende, se informa que el control se encuentra operando correctamente.

14	Gestión de Emergencias.	2	El Grupo Operaciones C-4, mensualmente verifica la disponibilidad de personal asignado para el cumplimiento de las tareas dentro de la operación del NUSE123, de lo cual entregara una proyección sobre ausencia de personal y necesidades de operación. como evidencia se entregará matriz proyección de turnos operación de C4, para toma de decisiones. en caso de no contar con el personal necesario de operación envían un correo al jefe de C4, con la novedad.	La dependencia responsable remite matriz de proyección correspondiente al tercer cuatrimestre de la vigencia 2023, completamente diligenciada, por esto, se está cumpliendo con lo establecido en el control. Por otra parte, se sugiere sea revisado puntalmente el control actualmente establecido puesto que, el riesgo asociado a Pérdida de Confidencialidad, Integridad y/o disponibilidad de la información, no se cobijarían con el hecho de generar la matriz de proyección de turnos.
14	Gestión de Emergencias.	3	El grupo de entrenamiento C-4, semestralmente, realiza capacitación y /o sensibilización a funcionarios y contratistas sobre el correcto uso de contraseñas de acuerdo a lo establecido en el manual de seguridad y privacidad de la información de la Entidad, como soporte de la evidencia se dejaran 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.	Se validan los soportes de capacitaciones adelantadas en el último cuatrimestre de 2023, observando que se han realizado actividades propias sobre seguridad de la información, por tanto, el control se encuentra operando correctamente. No obstante, a lo anterior, se recomienda que los soportes asociados al control sean los específicos, puesto que se remitieron evidencias sobre la UPS, tema que no está relacionado directamente con las capacitaciones, es decir en el control; adicionalmente, se sugiere a la segunda línea de defensa que previo a los reportes cuatrimestrales, se realicen validaciones de los soportes remitidos por la primera línea.
15	Gestión de Emergencias.	1	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 Secretaria Distrital de Seguridad, convivencia y Justicia. Como evidencia se generan las actas del contratista del mantenimiento y los informes técnicos de funcionamiento de las UPS, en caso de no realizar los mantenimientos programados se deberá informar mediante correo electrónico sobre los motivos así como las acciones para cumplir con los mantenimientos. el cargue de evidencia se hará trimestralmente.	Se validan reportes mensuales emitidos por la dependencia responsable sobre los procesos o acciones realizadas sobre la UPS y la planta eléctrica en el C4. De acuerdo con lo mencionado el control se encuentra operando correctamente.

16	Gestión de Emergencias.	1	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 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.	Se evidencian los soportes remitidos y generados por la dependencia responsable en los meses de septiembre, octubre y noviembre de 2023, tal y como se describe en el control, por medio del documento conciliación técnica mensual.
16	Gestión de Emergencias.	2	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.	Se evidencian informes mensuales y de supervisión del contrato 1932 de 2023 correspondientes a los meses de septiembre, octubre y noviembre, de acuerdo con lo conceptuado en el control; en estos se evidencia capitulo donde se trata el tema de los acuerdos de niveles de servicios ANS.
17	Gestión de Emergencias.	1	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.	La dependencia responsable remite informes mensuales de actividades desde agosto a noviembre de 2023, asociados al contrato 1611 de 2023 en referencia al sistema de radio comunicaciones distrital. Dentro de estos se observa un ítem relacionado con los acuerdos de niveles de servicio que para el reporte de noviembre-diciembre fue cumplido por parte del contratista. Por lo anterior, el control se encuentra operando correctamente.
18	Gestión de Seguridad y Convivencia.	1	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 equipo auditor evidencia dos soportes generados en el tercer cuatrimestre de 2023 asociados a la gestión de usuarios y roles dentro del sistema de información Progressus, así como también el reporte al líder de la dependencia, por esto el control se encuentra operando correctamente.

18	Gestión de Seguridad y Convivencia.	2	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.	La dependencia responsable remite soporte de publicación en portal MIPG de la guía para el registro y validación de actividades en progressus. Adicionalmente, se valida en portal MIPG que la fecha de publicación de la guía en mención fue el 29 de diciembre de 2023. Ante lo descrito, el control se encuentra operando correctamente. Derivado de lo anterior y al haber publicado oficialmente la guía, se recomienda al proceso responsable, se evalúe la actualización del control por medio de una nueva actividad complementaria asociada, que de fe de la adopción y el cumplimiento de lo establecido en la guía.
19	Gestión de Seguridad y Convivencia.	1	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.	Se observan dos actas de reunión generadas en el cuatrimestre por parte del proceso responsable, donde específicamente se trata el tema del riesgo 19 control 1, donde se realiza seguimiento y revisión del archivo documental y también en lugar que tiene alojada la información de carácter importante. Lo anterior bajo lineamientos de la Directora de Seguridad, por ende el control se encuentra operando correctamente.
20	Gestión de Seguridad y Convivencia.	1	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.	La dependencia responsable remite documentos soporte mensuales generados en el tercer cuatrimestre de 2023, donde se validan las actas generadas en los consejos locales de seguridad, identificando la información de carácter sensible y reportándolo a los diferentes equipos, por tal motivo, el control se está ejecutando correctamente.
21	Gestión de Seguridad y Convivencia.	1	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	Se evidencia correo electrónico remitido en noviembre por la dependencia responsable donde se solicita al equipo el diligenciamiento y ajuste de los registros vinculados al formulario, por lo anterior, el control está operando correctamente.
22	Gestión de Seguridad y Convivencia.	1	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.	Se evidencia archivo con el análisis de registros correspondientes a los meses de octubre y noviembre en la dependencia responsable, los cuales arrojan resultados por encima del 80% de correspondencia. No obstante, después de validado el soporte, se recomienda a la segunda línea de defensa incluir los evidencias de todo el cuatrimestre de acuerdo con su corte, para poder concluir que el control se está ejecutando continuamente.

23	Gestión de Tecnologías de la Información.	1	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.	La dependencia responsable remite actas de los sistemas de información, Simba, encuesta telefónica, botón sordos y Progressus. Para fortalecer la operación del control, nos permitimos recomendar que se adicionen a los soportes, los planes de trabajo de todos los sistemas de información que se encuentren en desarrollo o ajuste, con el fin de determinar a cuales efectivamente se le realizó el seguimiento tal y como lo estipula la descripción del control.
23	Gestión de Tecnologías de la Información.	2	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	Los soportes o evidencias remitidos por la dependencia responsables son el manual de LICO y el manual de desarrollo seguro con fecha diciembre de 2023. Si bien el control define que se deben remitir los manuales técnicos actualizados, en primera instancia nos permitimos informar una oportunidad de mejora por el hecho de no remitir los manuales de TODOS los sistemas de información y en segunda medida, no se evidencia soporte que dé cumplimiento del seguimiento a la ejecución del plan de actualización documental de la arquitectura de los sistemas de información, tal y como se describe en el control.
24	Gestión de Tecnologías de la Información.	1	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 contara 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.	La dependencia responsable remite el manual de seguridad y privacidad de la información y un documento sobre la gestión de credenciales. Sin embargo, no se entregan soportes de seguimiento que se realiza trimestralmente al cumplimiento de los mecanismos y/o la comunicación formal con las alternativas adoptadas dirigida al Director de la DTSI, por lo anterior, los soportes del control se encuentran incompletos para lo cual se sugiere que para el siguiente seguimiento, se generen los soportes tal y como lo describe el control.

24	Gestión de Tecnologías de la Información.	2	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.	La DTSI remite evidencias con la propuesta del plan de contingencia tecnológico, bitácora de actividades apagado de data center y bitácora de migración de bases de datos realizados en el tercer cuatrimestre de la vigencia. No obstante a lo anterior, se recomienda puntualizar las evidencias a generar frente a: como se garantiza la disponibilidad reduciendo el riesgo de depender de un único proveedor de nube, así como también realizar validación del control actualmente establecido, puesto que está asociado al plan de contingencia de servicios tecnológicos y este documento aún no ha sido formalizado en la plataforma MIPG, complementariamente, este control como está relacionado con la disponibilidad de servicios internos de TI, es importante incluirle los temas que actualmente se encuentran en operación dentro del C4.
24	Gestión de Tecnologías de la Información.	3	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.	Se remite por parte de la dependencia responsable evidencias mensuales sobre los análisis ejecutados a la seguridad perimetral de la entidad (seguridad informática), por lo cual se cumple con lo establecido en el control.
25	Gestión y Análisis de la Información.	1	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.	Se evidencia hoja de vida del indicador actualizado a diciembre de 2023, con el cual se cumple lo definido en el control.
26	Evaluación al Sistema de Control Interno.	1	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	No se tienen cargados soportes de ejecución de control dentro del repositorio de información puesto que no se presentaron eventos y este no se ejecutó en el tercer cuatrimestre de 2023.

26	Evaluación al Sistema de Control Interno.	2	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 presentara el comunicado oficial enviado y las respuestas de las procesos y/o dependencias.	Se evidencian documentos memorandos con el cual se solicita a las dependencias los enlaces responsables del diligenciamiento del plan de mejoramiento institucional, por lo anterior para la vigencia 2023 se cumplió con lo determinado dentro del control.
27	Evaluación al Sistema de Control Interno.	1	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 solicitara a la DTSI se genere el reporte correspondiente por parte del administrador de la herramienta.	Se evidencian soportes del cumplimiento del control en el mes de diciembre de 2023 de acuerdo de lo estipulado.
28	Sin Proceso	1	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.	Se evidencia ejecución del control de acuerdo a lo establecido para el mes de noviembre de 2023, sin embargo, se recomienda validar el control en su totalidad, puesto que los documentos (actas), se están almacenando en OneDrive de una cuenta puntual y al momento de la emisión de este informe, la persona encargada no tiene vínculo con la Entidad, por tanto se puede presentar un riesgo de disponibilidad.

Tabla N°. 6. Elaboración Propia. Fuente Matriz de riesgos de seguridad de la información F-FI-1385 V1.

Una vez culminado el análisis de los controles por parte del equipo auditor, a continuación, se resaltan los temas a mejorar de manera general así:

- ⚠ Generar soportes puntuales de acuerdo con lo descrito dentro del control.
- ⚠ Complementar evidencias documentales descritas en el control que den fe principalmente de actividades de revisión o monitoreo.
- ⚠ Inclusión de nuevas actividades de control que complementen o aborden el riesgo con mayor impacto.
- ⚠ Monitoreo de la ejecución de los controles por parte de la segunda línea de defensa.
- ⚠ Formalización de documentos en el sistema integrado de gestión.

5. CONCLUSIONES

- ✓ Se resalta la importancia de asociar aspectos tales como inventarios de activos de información, riesgos y controles al mapa de procesos V.2 de la entidad, puesto que no se está cubriendo la totalidad de estos, generando riesgos de confidencialidad, disponibilidad e integridad de la información.

- ✓ La segunda línea de defensa tiene un papel preponderante, debido a su experticia y conocimiento del tema, por tanto, se requiere que esta asesore a todas las dependencias y procesos en la generación de nuevos controles y/o actividades de acuerdo con la dinámica que los riesgos de seguridad de la información presentan tanto a nivel externo como interno y debido a la evolución de las amenazas. De igual manera, a modo de oportunidad de mejora, se enfatiza en la validación de los soportes que la primera línea comparte, para garantizar la consistencia y asociación a lo descrito en la estructura del control.

Elaboró

Diego Alexander Urazán Franco
Contratista Oficina de Control Interno

Reviso y Aprobó:

Karol Andrea Parraga Hache
Jefe Oficina de Control Interno