ALCALDÍA MAYOR DE BOGOTÁ
SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA
AL RESPONDER CITAR EL NR.
Nro. Rad: 3-2023-21506
Fecha: 07/06/2023 07:07:08 PM - Anexos:
Destino: 100-DESPACHO

MEMORANDO

Para: OSCAR ANTONIO GOMEZ HEREDIA
DESPACHO SECRETARIO DE SEGURIDAD

De: OFICINA DE CONTROL INTERNO

Asunto: INFORME DE SEGUIMIENTO A CONTROLES ASOCIADOS A RIESGOS DE SEGURIDAD DIGITAL - PRIMER CUATRIMESTRE DE 2023

Cordial saludo, Doctor Gómez Heredia:

De conformidad con los roles asignados a esta Oficina en cumplimiento del artículo 17 del Decreto 648 de 2017, así como al Plan Anual de Auditoria vigencia 2023 y la Política de Administración de Riesgos Versión 7 de la Secretaría, me permito presentar el informe de seguimiento a controles asociados a riesgos de seguridad digital para el primer cuatrimestre de 2023.

Esta oficina emite este informe, como insumo para la aplicación de las recomendaciones dadas en pro del fortalecimiento en la administración del riesgo e identificación de acciones que permitan aportar en el mejoramiento continuo.

Cordialmente,

KAROL ANDREA PARRAGA HACHE
JEFA OFICINA DE CONTROL INTERNO

c.c.e.: IVAN HERSAYN PINILLA HERRERA-DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION
JUAN DAVID GARCIA RUEDA-OFICINA ASESORA DE PLANEACION
Anexo: N/A
Anexos Digitales: 1

Elaboró: DIEGO ALEXANDER URAZAN FRANCO-OFICINA DE CONTROL INTERNO
Revisó: ANDREA DEL PILAR ALEJO RUIZ-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 Digital.

I Cuatrimestre de 2023

Oficina de Control Interno

SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA

BOGOTÁ

Tabla de contenido

1. OBJETIVO.

Evaluar dentro de la Entidad la adecuada implementación y diseño de los controles a través de los cuales se gestionan los riesgos de seguridad digital, con corte 30 de abril de 2023, de acuerdo con la versión 07 de la Política de Administración de Riesgos de la Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ.

2. ALCANCE.

La evaluación se enmarcó en el diseño y ejecución de los controles reportados por la Primera Línea de Defensa correspondiente al primer cuatrimestre de la vigencia 2023 dentro de la Matriz General de Riesgos de Seguridad Digital F-DS-898 y los soportes de ejecucion de estos.

3. METODOLOGÍA.

- ✓ Notificación a la Oficina Asesora de Planeación (en adelante OAP) por parte de la Oficina de Control Interno (en adelante OCI) del seguimiento a realizar.
- ✓ 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 (DTSI) y consultada en el SharePoint donde se alojan las evidencias de ejecución de los controles.

4. RESULTADOS.

De acuerdo con el objetivo planteado para este seguimiento, a continuación, se presentan los siguientes resultados:

4.1. Aplicación de la metodología registrada en la política de administración de riesgos de la Entidad.

4.1.1. Etapa 1: Conocimiento de la actual Política de Administración de Riesgos:

Vía correo electrónico el día 2 de marzo de 2023 se divulgó a toda la Entidad una pieza comunicativa invitando a los colaboradores a consultar la matriz de riesgos de seguridad digital así:

Imagen N°. 1. Fuente: Correo electrónico con pieza comunicativa generada por la DTSI y remitida el 2 de marzo de 2023.

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

Para la vigencia 2022, la Entidad en cabeza de la Dirección de Recursos Físicos y Gestión Documental y la Dirección de Tecnologías y Sistemas de la Información, desarrolló un proceso de levantamiento de activos de información en todas las dependencias, tema culminado y publicado en la página web de la Secretaría.

Para la vigencia 2023 y debido a la actualización del mapa de procesos que se está realizando, aun no se ha iniciado la actualización del inventario de activos de información, tema que debe abordarse anualmente. Expuesto lo anterior y para que exista concordancia de información, se recomienda dar celeridad a la actualización del inventario, puesto que hay que ejecutar todas las fases para los nuevos procedimientos.

Derivado de los datos publicados en página web con corte a primer cuatrimestre de 2023 y partiendo de un total de 331 activos de información identificados y formalizados en la Entidad, de acuerdo con la valoración de la criticidad para cada uno de estos, en nivel alto se catalogaron 79 activos, seguidos de 164 en nivel medio y finalmente 88 con nivel bajo. A continuación, se presenta la gráfica con el detalle de lo mencionado:

Gráfico N°. 1. Elaboración Propia. Fuente: Página Web SCJ – Registro de activos de información e indice de información clasificada y reservada.

Por otra parte, se observó que el registro de activos de información e índice de información clasificada y reservada se encuentra actualizado y publicado en la página de la Secretaría dentro de la sección de transparencia con fecha 14 de diciembre del 2022:

Imagen N° 2 Fuente Pagina Web SCJ - Publicación registro de activos de información

4.1.3. Etapa 3: Identificación del riesgo:

Para la identificación de riesgos en la matriz de seguridad digital, a cada activo de información se le aplicó una valoración respecto a los pilares de seguridad de la información: confidencialidad, disponibilidad e integridad de acuerdo con la afectación; así mismo dentro de estos se hizo el análisis de vulnerabilidades y amenazas para la correspondiente aplicación de controles.

4.1.4 Etapa 4: Valoración del riesgo:

Para la valoración del riesgo y de acuerdo con la política de administración de riesgos, se debe calcular la probabilidad y el impacto así:

Probabilidad: Se tienen definidos los siguientes niveles:

Tabla Criterio de Probabilidad

Nivel de Probabilidad	Frecuencia de la actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximo 1 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 2 a 1.000 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 1.001 a 5.000 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 5.001 veces al año y máximo 10.000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 10.001 veces por año	100%

Imagen N° 3 Fuente Política De Administración Del Riesgo

Impacto: Cuenta con los siguientes niveles:

Tabla Criterio de impacto

Niveles de Impacto	Afectación Económica	Afectación Reputacional	Impacto
Leve	Afectación menor a 49.999 SMLMV	El riesgo afecta la imagen de algún área de la organización.	20%
Menor	Entre 50.000 y 99.999 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.	40%
Moderado	Entre 100.000 y 199.999 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.	60%
Mayor	Entre 200.000 y 299.999 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.	80%
Catastrófico	Mayor a 300.000 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país	100%

Imagen N° 4 Fuente Política De Administración Del Riesgo

De acuerdo con lo anteriormente expuesto y al contrastarlo contra la matriz de riesgos de seguridad digital, se están utilizando únicamente 3 niveles en probabilidad y 3 niveles en Impacto así:

Imagen N° 5 Matriz de riesgos de seguridad digital.

Lo anterior indica que no se están usando los niveles Alta y Muy alta para probabilidad; y menor y catastrófico para Impacto, de acuerdo con la valoración otorgada para cada uno de los procesos.

Continuando con el proceso, el siguiente paso consiste en el tratamiento de riesgos, el cual se cataloga en 3 ítems:

- Aceptar el riesgo
- Reducir el riesgo
- Evitar el riesgo

Complementariamente a la anterior clasificación, en la matriz de riesgos de seguridad digital en la parte titulada tratamiento de riesgos dentro de la columna etiquetada como tipo de acción acorde a lo definido en la Política de Administración de Riesgos, se observa en su totalidad la tipología "reducir el riesgo", es decir, no han establecido controles apuntando a otra tipología como "evitar el riesgo".

4.1.5 Etapa 5: Creación de controles:

Dentro de la matriz de riesgos de seguridad digital a cada uno de los riesgos identificados se le asocia uno o varios controles incorporando la estructura del control así: responsable (adecuado), evidencias, fuentes de información, desviaciones u observaciones y periodicidad, entre otros campos. No obstante, no se observó el campo relacionado con el objetivo del control tal como lo define el numeral 10.7.1 de la política de administración de riesgos de la Entidad. Por tanto, es necesario validar los campos de información de la matriz vs lo establecido en la política a fin de alinear la información para todas las herramientas.

4.1.5.1 Evaluación de la estructura de controles:

Se evaluó la estructura de los controles tal y como se define en los lineamientos del numeral 10.7.1 de la política de administración del riesgo de la Secretaría, obteniendo los siguientes resultados:

- **Tener un responsable de ejecución**: Al revisar la matriz de riesgos de seguridad digital en la hoja **TRATAMIENTO DE RIESGO,** se observa una columna titulada *"responsable de control"* donde el único valor que se carga es asignado, y no se registra un responsable propiamente; no obstante, en el campo *"nombre del control"* se mencionan los responsables, sin embargo, en los siguientes casos esta definición no tiene claridad así:

N° Riesgo	N° Control	Proceso	Nombre de Control	Observación OCI
2	1	Acceso y Fortalecimiento de la Justicia	Los responsables de la Dirección de acceso a la justicia asignado, trimestralmente verifica los permisos de derecho de acceso a los diferentes	No se describe claramente quien es el responsable de la ejecución del

N° Riesgo	N° Control	Proceso	Nombre de Control	Observación OCI
			formularios, 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 del área 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 área.	control y si este cuenta con la segregación de funciones, como lo recomienda la Política.
11	1	Gestión Humana	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	Según el control esta tarea esta asignada al equipo de nómina, por tanto, no tiene un responsable especifico, tema que es ejecutado por la profesional especializada del área.

Tabla N°. 1. Elaboración Propia. Fuente: matriz de riesgos de seguridad digital F-DS-898

- **Especificar como se ejecuta la acción del control:** Frente a este aspecto la totalidad de controles cumplen con el llamado a la acción.

- **Soporte documental:** Frente a esta condición se menciona que el **control 1 del riesgo 25 asociado al proceso Gestión y Análisis de la Información de S,C y AJ** no define claramente el soporte o evidencia documental que se debe generar. El control describe: *"El responsable de la bodega de datos realiza actualizaciones de información recibida por parte de fuentes internas y externas, la cual se valida por medio de una consulta SQL a la base de datos cuyo resultado es evidenciado en el indicador de gestión" cumplimiento en la actualización de la bodega de datos" el cual es reportado periódicamente a la OAP. En caso de incumplimiento de este indicador se deberá realizar la justificación pertinente en el portar MIPG."*

- **Periodicidad de la aplicación:** Esta condición tampoco es cumplida para el control **1 del riesgo 25 asociado al proceso Gestión y Análisis de la Información de S,C y AJ**, informado en el ítem anterior.

- **Objetivo: El control 2 del riesgo 18 asociado al proceso de Gestión de Seguridad y Convivencia** define *"El responsable de gestión de la información de Subsecretaría de seguridad y convivencia liderará 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 y que será validada por el líder del proceso; una vez construida la guía se actualizará y divulgará semestralmente a través de correo electrónico a los líderes de equipo para su debida implementación."* De acuerdo con la validación realizada, este control no cuenta con un objetivo tal como lo estipula la política (*"La definición debe incluir cuál es el Objetivo del control (valida, coteja, compara, concilia…"*).

- Desviaciones entre el resultado esperado y el resultado obtenido: El control 1 del riesgo 9 del proceso de Gestión Humana define: *"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, como evidencia se tendrán las comunicaciones de solicitud y retiro de acceso de usuarios. el cargue de evidencia se realizará Semestralmente"*. Para tal fin, no se tiene claridad sobre la desviación, ya que la política determina que "*desviaciones entre el resultado esperado y el resultado obtenido y que acciones se deben tomar si se presentan dichas desviaciones*."

Observación N°1: Una vez validado el diseño de los controles registrados dentro de la matriz de riesgos de seguridad digital, respecto a lo definido en la política de administración de riesgos versión 7 de la Entidad, para 4 procesos (ver numeral anterior) se presentan debilidades frente a los lineamientos de diseño que cada uno de estos debe cumplir. Lo anterior indica que el 14 % de los controles presentan novedades.

4.1.6. Etapa 6: Tratamiento de riesgo residual:

El tipo de acción para el tratamiento de riesgo residual se encuentra catalogado y alineado entre la matriz de riesgos de seguridad digital y la política de administración del riesgo numeral 12.6. Informando específicamente que de acuerdo con las valoraciones realizadas dentro de la Entidad se están utilizando las tipologías de acciones reducir, evitar y compartir los riesgos.

4.1.7: Etapa 7: Monitoreo, revisión y reporte de la Gestión de Riesgos de Seguridad de la Información:

La matriz de riesgos de seguridad digital se encuentra actualizada para la vigencia 2023 de acuerdo con las fechas de implementaciones de los controles en la hoja tratamiento de riesgo residual. Adicionalmente y como lo define la Política de administración de riesgos de la Entidad, se está cumpliendo lo allí estipulado en ítems tales como:

- ✓ Definición de acciones de control para el manejo de riesgo.
- ✓ Responsable del proceso de verificación de los controles.
- ✓ Seguimiento de riesgos de manera cuatrimestral informando que este es el primer seguimiento que se realiza por parte de la segunda y tercera línea de defensa.

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

La matriz de riesgos de seguridad digital de la SDSCJ actualmente se compone de 28 riesgos, los cuales tienen asociados 36 controles clasificados por proceso así:

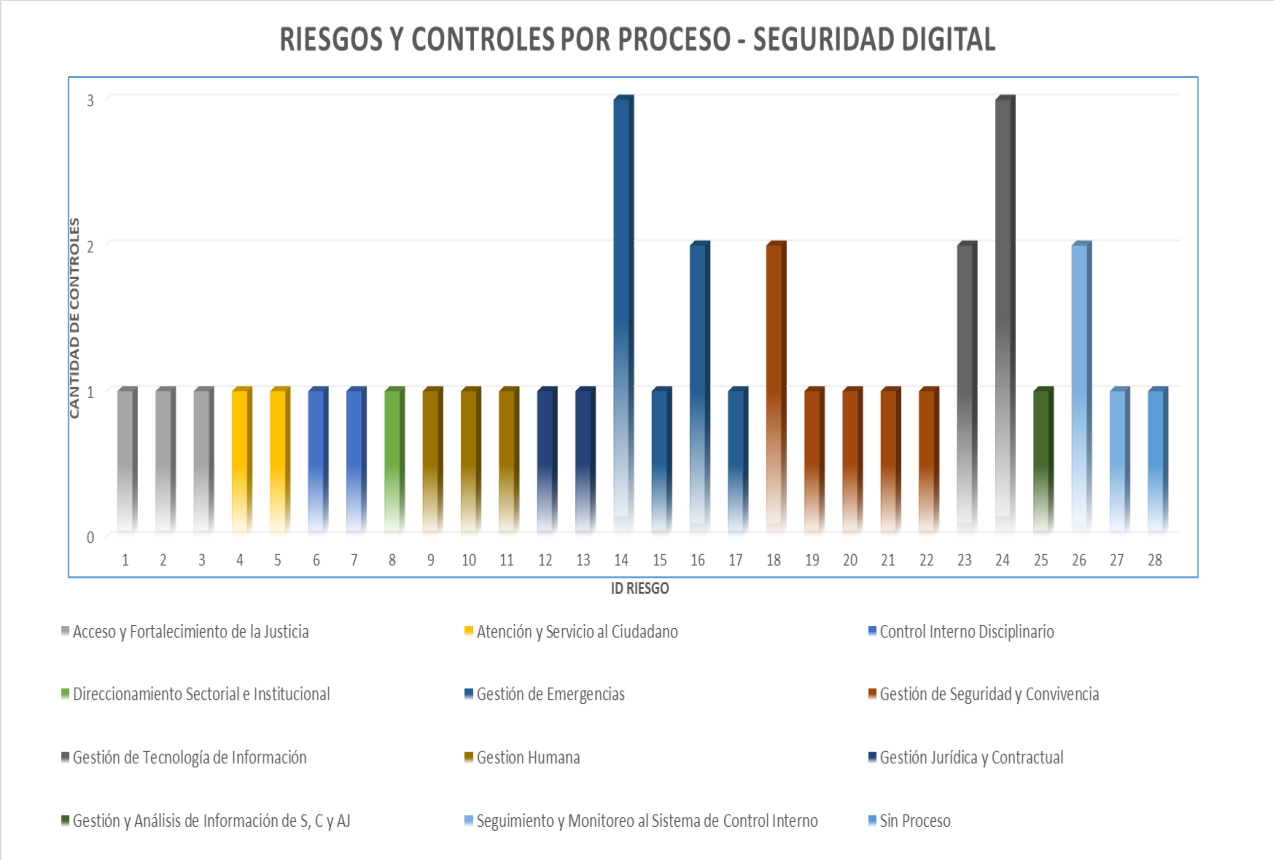


Gráfico N° 2 Elaboración propia. Fuente Matriz de riesgos de seguridad digital.

Lo anterior indica que los riesgos con mayor número de controles construidos y asociados son los números 14, 16, 18, 23, 24 y 26, los demás riesgos tienen asociados únicamente un control. De otro lado, se recomienda identificar el nombre del proceso asociado al riesgo No 28, ya que en la matriz se cataloga como "Sin proceso".

Luego de la evaluación realizada a la ejecución de los controles, se obtuvieron los siguientes resultados:

Código Riesgo	Proceso	Control	Seguimiento OCI	Recomendación
1	Acceso y Fortalecimiento de la Justicia	Los responsables de la generación de la información (funcionarios públicos y/o contratistas) entregan de acuerdo a la naturaleza de los documentos (mensual - trimestral -semestral y anual) al Director de la Dirección de Acceso a la Justicia los soportes relacionados a estos activos. En caso que no se realice la entrega de los documentos en los tiempos establecidos, el Director de DAJ solicitara a los responsables la entrega oportuna de la información sopena del incumplimiento de metas, requerimientos internos y externos; como evidencia quedaran los soportes de la documentación entregada en los	Se evidencian 5 soportes donde se solicita por parte del profesional Universitario a los responsables, la información sobre metas de la dependencia.	No aplica

Código Riesgo	Proceso	Control	Seguimiento OCI	Recomendación
		repositorios SharePoint disponibles para el área.		
2	Acceso y Fortalecimiento de la Justicia	Los responsables de la Dirección de acceso a la justicia asignado, trimestralmente verifica 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 enviara comunicación oficial y/o correo electrónico al Jefe del área 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 área.	Dentro de los soportes entregados por el responsable de la ejecución del control, se evidenció un correo electrónico en el cual se reporta a la Directora de la dependencia la verificación de los permisos a los formularios. No obstante, el control estipula que se deben generar datos acerca de los usuarios que cuentan con acceso y el tipo de acceso a la información, retirando el acceso a los que no lo requieren, todo esto debe contar con la aprobación de la Directora. Por lo mencionado, el control no se está ejecutando de acuerdo con lo definido.	Cumplir a cabalidad lo estipulado dentro del control, consistente en el reporte trimestral de todos los usuarios que tienen acceso a la información con sus privilegios y la correspondiente respuesta de aceptación o eliminación por parte de la Directora.
3	Acceso y Fortalecimiento de la Justicia	El profesional de acceso a la Justicia asignado, tendrá a su cargo las llaves del archivador de documentos, contará con una lista de personas autorizadas al acceso de la información, dicha información se revisará trimestralmente y en caso que se requiera se generará la solicitud de autorización. 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 SAJ, una vez sea autorizada, se debe dejar correo electrónico para efectos de trazabilidad.	De acuerdo con el soporte entregado por la dependencia responsable de la ejecución del control, se informa no existe un archivador para la documentación, por tanto, el control tal como está diseñado no se ejecuta.	Actualizar el control de acuerdo con la realidad operativa del proceso, debido a que no se tiene un archivador para el depósito de documentos.
4	Atención y Servicio al Ciudadano	Trimestralmente el responsable del registro documental realiza verificación de información recibida por parte de fuentes internas y externas validando la integridad de la información. y alimentando con la información los formatos que sean necesarios. 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 observan soportes de ejecución del control asociado a lo definido.	No aplica
5	Atención y Servicio al Ciudadano	El responsable de la oficina 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	Se evidencia el reporte de los usuarios activos en el sistema COPE; No obstante, y validando lo estipulado dentro del control, no se encuentran soportes donde se solicite la información a la DTSI	Complementar los soportes o evidencias de la ejecución del control de acuerdo con lo

Código Riesgo	Proceso	Control	Seguimiento OCI	Recomendación
		acuerdo a los roles y responsabilidades asignados, como soporte de la revisión enviara comunicación oficial y/o correo electrónico solicitando el envío de información y la respuesta requerida al personal encargado, en caso que exista usuarios no autorización se solicita retirar los permisos de acceso e informar las actividades realizadas.	(esto para constatar la fecha de ejecución del control) y la comunicación complementaria en donde se solicite la activación o inactivación de usuarios.	estipulado en el diseño.
6	Control Interno 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.	Se evidencia soporte de ejecución del control tal como se estipula en el diseño.	No aplica
7	Control Interno Disciplinario	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 soporte de ejecución del control tal como se estipula en el diseño.	No aplica
8	Direccionamiento Sectorial e 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,	Se evidencia soporte de ejecución del control tal como se estipula en el diseño.	No aplica
9	Gestión Humana	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	Teniendo en cuenta que el proceso establece el cargue de las evidencias semestralmente, para este periodo de seguimiento, este	Ejecutar el control por parte de la dependencia

Código Riesgo	Proceso	Control	Seguimiento OCI	Recomendación
		repositorios asignados para el manejo de esta información, como evidencia se tendrán las comunicaciones de solicitud y retiro de acceso de usuarios. el cargue de evidencia se realizara Semestralmente	control no contó con evidencia para la evaluación.	responsable tal cual como está definido, monitoreando los usuarios responsables que tienen acceso a los repositorios de información y realizando la respectiva depuración.
10	Gestión Humana	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 realizara Semestralmente	Teniendo en cuenta que el proceso establece el cargue de las evidencias semestralmente, para este periodo de seguimiento, este control no contó con evidencia para la evaluación.	Ejecutar el control por parte de la dependencia responsable tal cual como está definido, donde se relaciona la base de datos de préstamos de historias laborales.
11	Gestión Humana	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 realizara Semestralmente	Teniendo en cuenta que el proceso establece el cargue de las evidencias semestralmente, para este periodo de seguimiento, el control no contó con evidencia para la evaluación.	Generar los soportes documentales tal como lo estipula el control por parte de la dependencia responsable y de acuerdo con la periodicidad definida.
12	Gestión Jurídica y 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.	Se evidencia soporte de ejecución del control tal como se estipula en el diseño para la vigencia 2023.	No aplica
13	Gestión Jurídica y Contractual	El responsable del equipo de archivo de la Dirección Jurídica y Contractual anualmente realiza la intervención documental de los expedientes en	Se evidencia soporte de ejecución del control tal como se estipula en el diseño en la vigencia 2023.	No aplica

Código Riesgo	Proceso	Control	Seguimiento OCI	Recomendación
		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.		
14	Gestión de Emergencias	El responsable del proyecto NUSE123, verifica el informe de seguimiento a la operación entregado de forma mensual por la empresa ETB y realiza mensualmente los reportes al Jefe C-4 de las novedades, hallazgos y/o recomendaciones entregadas. como evidencia se entregará comunicado oficial sobre el seguimiento a la operación y las acciones realizadas, en caso de no contar con el reporte que entrega la empresa ETB, se realizaran las gestiones pertinentes mediante comunicado oficial y/o correo electrónico sobre la solicitud de información.	Los soportes documentales entregados por el responsable de la ejecución del control son los informes mensuales de interventoría que remite el contratista, no obstante, el control describe que el responsable del proyecto en el NUSE remite a la Jefatura del C4 reporte con las novedades, hallazgos y/o recomendaciones entregadas.	Puntualizar y generar los soportes tal y como lo describe el control y si aplica realizar el ajuste en la descripción del control.
14	Gestión de Emergencias	Grupo Operaciones C-4, mensualmente verifica la disponibilidad de personal asignado para el cumplimiento de las tareas dentro de la operación del NUSE123, de lo cual entregara una proyección sobre ausencia de personal y necesidades de operación. como evidencia se entregará matriz proyección de turnos operación de C4, para toma de decisiones. en caso de no contar con el personal necesario de operación envían un correo al jefe de C4, con las novedad.	Se evidencian soportes de ejecución del control tal como este lo define. (Soportes de enero a abril de 2023)	No aplica
14	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 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 evidencian soportes (Capacitaciones, evaluaciones y sensibilizaciones respecto a seguridad de la información) de ejecución del control tal como se tiene definido.	Identificar dentro de los soportes de ejecución del control, los procesos de capacitación o sensibilización directamente relacionados con el tema de seguridad y privacidad de la información de la Entidad y específicamente al tema de contraseñas, tal

Código Riesgo	Proceso	Control	Seguimiento OCI	Recomendación
				como el control lo señala. De ser necesario evaluar la viabilidad de incluir en el control temas adicionales relacionados con seguridad de la información.
15	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 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 evidencian soportes de ejecución del control tal como este lo define. (Soportes de enero a abril de 2023)	No aplica
16	Gestión de Emergencias	El responsable del seguimiento del contrato de mantenimiento de videovigilancia, supervisa los mantenimientos externos a los equipos activos del sistema de videovigilancia, como evidencia se debe dejar la solicitud de cambio aprobada, correo electrónico de asignación de responsable, y los informes de las actividades desplegadas, en caso de no contar con personal disponible de acompañamiento a la visita, no se autorizará el ingreso al personal externo y se reprogramará el mantenimiento. El cargue de evidencia se entregara trimestralmente.	Se evidencian soportes de ejecución del control tal como este lo define. (Soportes de Enero a Marzo de 2023)	No aplica
16	Gestión de Emergencias	El jefe del C4 delega a la empresa contratista el mantenimiento y operación del sistema de videovigilancia. Estas actividades se registran en informes de gestión de la empresa contratista recibidos de forma mensual evidenciando la operación del sistema de videovigilancia controlada por ANS, que en caso de estar por debajo de umbral se penaliza económicamente. las Evidencia	Se evidencian soportes de ejecución del control tal como este lo define. (Soportes de Enero a marzo de 2023). Sin embargo, El control describe: "*Estas actividades se registran en informes de gestión de la empresa contratista recibidos de forma mensual evidenciando la operación del sistema de videovigilancia controlada por*	Adjuntar y complementar los soportes que evidencien el cumplimiento del control, específicamente las decisiones tomadas o las acciones ejecutadas

Código Riesgo	Proceso	Control	Seguimiento OCI	Recomendación
		corresponde al Informe mensual de la empresa contratista. El cargue de las evidencias se hará trimestralmente.	*ANS, que en caso de estar por debajo de umbral se penaliza económicamente"*; por tanto y para soportar la ejecución del control, las evidencias presentadas corresponden al informe mensual que genera la empresa contratista; de acuerdo con lo anterior, dentro de los soportes validados no se mencionan resultados o situaciones derivados del análisis de los ANS.	frente a los análisis de los ANS.
17	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.	Se evidencian soportes de ejecución del control tal como este lo define. (Soportes de Enero a marzo de 2023). Sin embargo, El control describe: "*Estas actividades se registran en informes de gestión de la empresa contratista recibidos de forma mensual evidenciando la operación del sistema de videovigilancia controlada por ANS, que en caso de estar por debajo de umbral se penaliza económicamente"*; por tanto y para soportar la ejecución del control, las evidencias presentadas corresponden al informe mensual que genera la empresa contratista; de acuerdo con lo anterior, dentro de los soportes validados no se mencionan resultados o situaciones derivados del análisis de los ANS.	Adjuntar y complementar los soportes que evidencien el cumplimiento del control, específicamente las decisiones tomadas o las acciones ejecutadas frente a los análisis de los ANS.
18	Gestión de Seguridad y Convivencia	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	Se evidencian soportes de ejecución del control tal como este lo define. Sin embargo, se el soporte demuestra que la ejecución fue realizada en el mes de abril incumpliendo la periodicidad establecida.	Tener presente la frecuencia establecida, puesto que en 2023 el control se ejecutó en el mes de abril.

Código Riesgo	Proceso	Control	Seguimiento OCI	Recomendación
		de proceso mediante correo electrónico y/o comunicado oficial.		
18	Gestión de Seguridad y Convivencia	El responsable de gestión de la información de Subsecretaría de seguridad y convivencia liderará 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 y que será validada por el líder del proceso; una vez construida la guía se actualizará y divulgará semestralmente a través de correo electrónico a los líderes de equipo para su debida implementación.	Dentro de los soportes del control no se visualiza avance en el desarrollo de la guía para el uso adecuado de la plataforma que incluya lineamientos para el registro y verificación de la información.	Desarrollar y presentar el avance de la guía estipulada dentro del control para el siguiente cuatrimestre. Adicionalmente, se recomienda validar el control en cuanto a diseño, el cual debe cumplir la estructura tal y como lo define la política de administración de riesgos.
19	Gestión de Seguridad y Convivencia	El o La Directora de Seguridad garantizará que los documentos se almacenen en un sitio seguro dispuesto por la Entidad para restringir el acceso y uso únicamente para los usuarios autorizados, para ello evidenciará trimestralmente por medio de acta que el proceso de custodia y confidencialidad del documento final se realizó adecuadamente o de la aplicación de los correctivos necesarios, en caso de requerirse.	Se evidencia soporte de ejecución del control tal como este lo define, sin embargo, el soporte reportado fue emitido al final del cuatrimestre, es decir 30 de abril, es decir fuera de términos.	No obstante, al soporte del control presentado, esta Oficina recomienda tener en cuenta la frecuencia de ejecución la cual se estableció de manera trimestral.
20	Gestión de Seguridad y Convivencia	El responsable de validar las Actas de los Consejos Locales de Seguridad en la plataforma dispuesta, verificara 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.	Se evidencia soporte de ejecución del control tal como este lo define.	No obstante, al soporte del control presentado, esta Oficina recomienda tener en cuenta la frecuencia de ejecución el cual está establecido mensualmente, por tanto, dentro de los soportes que se remiten para

Código Riesgo	Proceso	Control	Seguimiento OCI	Recomendación
				certificar el cumplimiento del control, se debe complementar con los soportes de los meses de enero, febrero y marzo de la presente vigencia.
21	Gestión de Seguridad y Convivencia	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 soporte de ejecución del control tal como este lo define.	No aplica
22	Gestión de Seguridad y Convivencia	"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 soporte de ejecución del control tal como este lo define.	No aplica
23	Gestión de Tecnología de Información	El responsable de sistema de información realiza seguimiento trimestral al cumplimiento del plan de actualización de entornos de desarrollo de los sistemas de información evidenciado en acta de aprobación, en caso de no contar con este reporte, se deberá dejar evidencia de las vulnerabilidades de cada sistema de información sobre la falta de actualización del entorno de desarrollo. Como evidencia de la ejecución del control se contará con el reporte de seguimiento al plan o con la verificación de versionamiento en el ambiente de desarrollo y producción	Se evidencia soporte de ejecución del control tal como este lo define.	No aplica
23	Gestión de Tecnología de Información	El responsable de sistema de información realiza seguimiento trimestral a la ejecución del plan de actualización documental de la	Se evidencia soporte de ejecución del control tal como este lo define. No obstante, solo se	Adjuntar todos los manuales de los sistemas de información tal

Código Riesgo	Proceso	Control	Seguimiento OCI	Recomendación
		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.	evidencia el manual del sistema de información SIGA.	como está definido dentro del control, o en su defecto adjuntar el reporte de seguimiento al plan.
24	Gestión de Tecnología de 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.	Se evidencia soporte de ejecución del control tal como este lo define.	No aplica
24	Gestión de Tecnología de Información	El responsable de infraestructura define el plan de recuperación de información en sitio alterno y reportara trimestralmente el seguimiento a la ejecución de las actividades del plan. en caso de no contar con el seguimiento trimestral a la ejecución del plan, se contará con comunicación formal al Director de Tecnologías informando las alternativas adoptadas. Como evidencia de la ejecución del control se contará con el plan de recuperación de información en el sitio alterno o comunicado formal.	Se evidencian soportes de ejecución del control. Sin embargo, el control estipula que se debe definir el plan de recuperación de información en sitio alterno.	Generar el plan de recuperación de información en el sitio alterno oficial de la Entidad, de acuerdo con lo definido en el control.
24	Gestión de Tecnología de 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.	Se evidencian soportes de ejecución del control tal como este lo define.	No aplica
25	Gestión y Análisis de	El responsable de la bodega de datos realiza actualizaciones de información recibida por parte de fuentes internas y	Se evidencian soportes de ejecución del control tal como este lo define.	No aplica

Código Riesgo	Proceso	Control	Seguimiento OCI	Recomendación
	Información de S, C y AJ	externas, la cual se valida por medio de una consulta SQL a la base de datos cuyo resultado es evidenciado en el indicador de gestión" cumplimiento en la actualización de la bodega de datos" el cual es reportado periódicamente a la OAP. En caso de incumplimiento de este indicador se deberá realizar la justificación pertinente en el portar MIPG.		
26	Seguimiento y Monitoreo 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	No se han generado solicitudes de acceso a información de usuarios en el presente cuatrimestre.	No aplica
26	Seguimiento y Monitoreo 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 presentará el comunicado oficial enviado y las respuestas de los procesos y/o dependencias.	Se evidencian soportes de ejecución del control tal como este lo define.	No aplica
27	Seguimiento y Monitoreo 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 solicitará a la DTSI se genere el reporte correspondiente por parte del administrador de la herramienta.	Se evidencian soportes de ejecución del control tal como este lo define.	No aplica
28	Sin Proceso	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	Se evidencian soportes de ejecución del control tal como este lo define.	No obstante, se considera importante asociar este riesgo y control al proceso que corresponda, a fin de dar

Código Riesgo	Proceso	Control	Seguimiento OCI	Recomendación
		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.		claridad respecto al impacto del mismo dentro de la gestión de la Entidad.

Tabla N°. 2. Elaboración Propia. Fuente: matriz de riesgos de seguridad digital F-DS-898

Como resultado de lo anterior, se expone que, de los 36 controles definidos, se tiene observación y comentarios sobre 13 de estos es decir el 36% en cuanto a la ejecución de estos.

Complementariamente, la Oficina de Control Interno, identificó que no todos los procesos tienen asociados controles de seguridad de la información dentro de los cuales se mencionan:

- Gestión de Comunicaciones.
- Fortalecimiento de Capacidades Operativas.
- Gestión Financiera.
- Gestión de Recursos Físicos y Gestión Documental.

4.3. Inconsistencias en las fechas establecidas para el Monitoreo, Seguimiento y Evaluación Matriz de Riesgos de Seguridad Digital, según Política de Administración de Riesgos bajo el esquema de líneas de defensa.

Durante el desarrollo de esta evaluación, esta oficina validó las fechas establecidas en la Política de administración de riesgos versión 7 de la Secretaría frente a los tiempos de ejecución de actividades por cada una de las líneas de defensa, como se detalla a continuación:

- Primera Línea: (Lideres de Procesos)
  Se requiere que los Líderes Operativos realicen el cargue de las evidencias a más tardar el 5° día hábil luego de vencido el Cuatrimestre.
- Segunda Línea: (Dirección de Tecnologías y Sistemas de la Información- Oficina Asesora de Planeación)
  Es responsabilidad del profesional de Seguridad de la Información de la Dirección de Tecnologías y Sistemas de la Información, realizar el seguimiento a la Matriz de Riesgos de Seguridad de la Información de manera cuatrimestral con el acompañamiento de la Oficina Asesora de Planeación, con un plazo de 10 días hábiles, una vez vencido el cuatrimestre, presentará un informe de gestión a la Oficina de Control Interno, responsable de la tercera línea de defensa.
- Tercera Línea: (Oficina de Control Interno)

Los cortes para realizar el seguimiento a la matriz de riesgos de **Seguridad de la Información** una vez se encuentre formulada, publicada, socializada e implementada son los siguientes:

FECHA DE CORTE	ENTREGA DEL INFORME
Primer corte: 30 de abril	Segunda semana de mayo
Segunda corte: 31 de agosto	Segunda semana de octubre
Tercer corte: 31 de diciembre	Segunda semana de febrero

Fuente: Elaboración propia

Imagen N° 6 Fuente Política de Administración de riesgos Versión 7

Una vez mencionado lo anterior, para las fechas de seguimiento y evaluación por parte de la segunda y tercera línea de Defensa se presenta una superposición, ya que la segunda línea tiene 10 días calendario para ejecutar seguimiento y entregar la información, tiempo que coincide con la fecha límite que tiene la Oficina de Control Interno para la evaluación (segunda semana de cada cuatrimestre), por tanto y al cruzarse estos tiempos, se presenta una probabilidad de incumplimiento de lo definido en la política respecto a los tiempos de evaluación.

Oportunidad de mejora N°1: Al cruzarse las fechas de seguimiento por parte de la Segunda Línea de Defensa (10 días hábiles, según numeral 15.3) y evaluación por la Tercera Línea de Defensa (Segunda semana, según numeral 15.6), existe probabilidad de no garantizar en oportunidad la publicación del informe respecto a lo establecido en la Política de Administración de Riesgos de la Entidad PO-DS-1 Versión 7.

5. CONCLUSIONES

- ✓ EL 14% de los controles, es decir 5 de los 36, presentan debilidades en su diseño al no cumplir con las características definidas en la Política de Administración de Riesgos de la Entidad Versión 7.

- ✓ Se presentó observaciones para 13 de los 36 controles, equivalente al 36%, asociadas a debilidades en la ejecución respecto de periodicidad definida, soportes documentales, realidad operativa y cumplimiento de lo establecido según su diseño.

- ✓ Se observó una adecuada organización de las evidencias documentales que soportan la ejecución de los controles registrados en la matriz de seguridad digital de la Secretaría.

- ✓ Por medio de los soportes evidenciados a través de correo electrónico, se observó gestión (socialización y alertamiento) por parte de la Dirección de Tecnologías y Sistemas de la Información frente a los riesgos de seguridad digital y seguridad de la información.

- ✓ Los inventarios de activos de información de la Secretaría no se encuentran actualizados en concordancia al nuevo mapa de procesos formalizado en la presente vigencia.

- ✓ A través de la evaluación realizada se identificó la necesidad de verificar las fechas establecidas para el monitoreo, seguimiento y evaluación que corresponde para cada una de las líneas de defensa según el Modelo Integrado de Planeación y Gestión.

6. RECOMENDACIONES

- Ejecutar un proceso de validación sobre la matriz de seguridad digital, específicamente en el uso y aplicación de todos los niveles de valoración de impacto y probabilidad, de acuerdo con lo estipulado en la política de administración del riesgo de la Entidad. En concordancia con lo

anterior, para el tratamiento de riesgo residual, es importante incluir un análisis con el objetivo de aplicar las otras tipologías de acción tales como evitar y compartir el riesgo.

- Validar y corroborar que todos los controles contenidos en la matriz de riesgos de seguridad digital estén alineados con el cumplimiento de los lineamientos de la política de administración de riesgos, no solamente en el tema de diseño de controles sino en los demás aspectos estipulados allí.

- Fortalecer el ejercicio de ejecución de los controles y reporte oportuno de los soportes documentales de acuerdo con lo que describe cada control, garantizando que las evidencias sean claras, de calidad y estén disponibles para consulta y verificación de los clientes internos que así lo requieran.

- Verificar por parte de la Primera y Segunda línea de Defensa la periodicidad de ejecución y cargue de evidencias para cada uno de los controles.

- Actualizar las fechas de ejecución de las actividades por parte de las Líneas de Defensa en la Política de Administración de Riesgos de la Entidad.

- Realizar actualización y unificación de conceptos, ya que se están mencionado tanto seguridad digital como seguridad de la información y en diversas fuentes se están utilizando los dos términos, por tanto, se pueden generar discrepancias frente a la terminología usada.

- Dentro de los procesos de revisión y actualización de la política de riesgos, es importante realizar un barrido determinando si todos los procesos tanto misionales como de apoyo y estratégicos deban tener por lo menos un control asociado a un riesgo de seguridad de la información, ya que transversalmente en toda la entidad se maneja (genera, procesa y envía) información y datos y por ende debe existir activos de información con carácter relevante para tener como resultado la adición de riesgos y controles. Lo anterior debe analizarse con base en la generación del nuevo mapa de procesos de la Entidad.

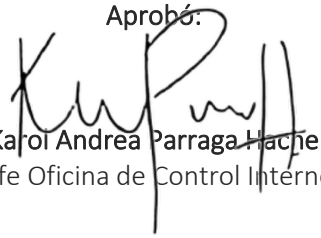
Elaboró

Diego Alexander Urazán Franco
Contratista Oficina de Control Interno

Revisó

Andrea del Pilar Alejo Ruiz
Contratista Oficina de Control Interno

Aprobó:



Karol Andrea Parraga Hache
Jefe Oficina de Control Interno