

### 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 CORRESPONDIENTE AL SEGUNDO 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 comunicar el informe de seguimiento a controles asociados a riesgos de seguridad digital correspondiente al **segundo** cuatrimestre de 2023.

Este informe se emite 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-OFCINA ASESORA DE PLANEACION

Anexo: 1

Anexos Digitales: 1

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



# Informe de Seguimiento a Controles asociados a los Riesgos de Seguridad Digital.

---

## II Cuatrimestre de 2023

Oficina de Control Interno



SECRETARÍA DE  
SEGURIDAD, CONVIVENCIA  
Y JUSTICIA



## Tabla de contenido

1.	OBJETIVO.....	3
2.	ALCANCE.....	3
3.	METODOLOGÍA.....	3
4.	RESULTADOS. ....	3
4.1.	Aplicación de la metodología registrada en la política de administración de riesgos de la Entidad.....	3
4.1.1.	Etapa 1: Conocimiento de la actual Política de Administración de Riesgos: .....	3
4.1.2.	Etapa 2: Identificación de los activos de seguridad de la información .....	4
4.1.3.	Etapa 3: Identificación del riesgo:.....	4
4.1.4	Etapa 4: Valoración del riesgo: .....	5
4.1.5	Etapa 5: Creación de controles: .....	6
4.1.5.1	Evaluación de la estructura de controles:.....	10
4.1.6.	Etapa 6: Tratamiento de riesgo residual: .....	12
4.1.7:	Etapa 7: Monitoreo, revisión y reporte de la Gestión de Riesgos de Seguridad de la Información: .....	12
4.2.	Matriz de riesgos de seguridad – Evaluación de Controles asociados a Riesgos .....	12
4.3.	Seguimiento aspectos por mejorar identificados en el primer cuatrimestre de 2023: .....	31
5.	CONCLUSIONES .....	32

## 1. OBJETIVO.

Evaluar y realizar seguimiento de la adecuada implementación y diseño de los controles a través de los cuales se gestionan los riesgos de seguridad digital, con corte 30 de agosto 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 segundo cuatrimestre de la vigencia 2023 dentro de la Matriz General de Riesgos de Seguridad Digital F-DS-898 y los soportes de ejecución 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.
- ✓ Inspección, validación y cotejo de evidencias.

## 4. RESULTADOS.

Una vez finalizada la revisión de los soportes remitidos por las dependencias responsables, nos permitimos compartir los siguientes resultados para el presente seguimiento:

### 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:

Respecto a la etapa de conocimiento, el día 15 de agosto de 2023, la DTSI, socializó a toda la Secretaría vía correo electrónico una pieza comunicacional sobre el **plan de tratamiento de riesgos de seguridad y privacidad de la información** así:

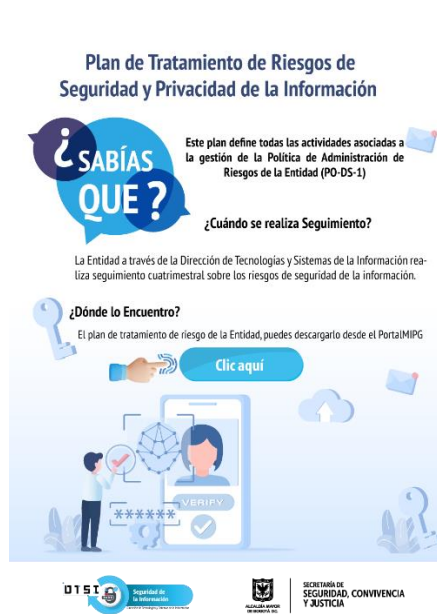


Imagen N° 1 Fuente correo electrónico remitido por la DTSI el día 15 de agosto de 2023

Adicionalmente, se cuenta con publicación de documentos en la intranet y en la página web de la entidad relacionados con riesgos de seguridad digital, tales como el plan de tratamiento de riesgos de seguridad, y privacidad de la información, la política y el manual de seguridad y privacidad de la información.

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

Para la vigencia 2023 no se ha ejecutado un proceso de actualización de activos de información, por lo que se continua con la versión de 2022, sin embargo, es importante tener en cuenta que, la actualización del mapa de procesos institucional conlleva la aparición/eliminación o actualización de los activos de información. Esta situación fue reportada en el anterior informe de seguimiento por parte de esta Oficina, sin que para el periodo objeto de este seguimiento se evidencien actividades tendientes a realizar la mencionada actualización.

Como se mencionó anteriormente, con corte a segundo cuatrimestre de 2023, se tiene 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.

#### 4.1.3. Etapa 3: Identificación del riesgo:

La matriz de riesgos de seguridad digital, al continuar en la misma versión tiene identificados 28 riesgos, los cuales están distribuidos por procesos de la siguiente manera:

Proceso	Cantidad de riesgos asociados
Acceso y Fortalecimiento a la Justicia	3
Atención y Servicio al Ciudadano	2
Control Interno Disciplinario	2
Direccionamiento Sectorial e Institucional	1
Gestión de Emergencias	4
Gestión de Seguridad y Convivencia	5
Gestión de Tecnología de Información	2
Gestión Humana	3
Gestión Jurídica y Contractual	2
Gestión y Análisis de Información de S, C y AJ	1
Seguimiento y Monitoreo al Sistema de Control Interno	2
Oficina de Despacho	1
<b>TOTAL</b>	<b>28</b>

Tabla N° 1 Elaboración propia. Fuente Matriz de riesgos de seguridad digital F-DS-898 V1.

De igual manera como se expresó en el informe de seguimiento correspondiente al primer cuatrimestre de la presente vigencia y puesto que no han variado, ni se han actualizado los riesgos y controles, se informa que los procesos con más riesgos de seguridad digital asociados e identificados son: Gestión de Seguridad y Convivencia, Gestión de Emergencias, Acceso y fortalecimiento a la Justicia y Gestión Humana.

**Oportunidad de Mejora N° 01: Falta de actualización de la matriz de riesgos de seguridad digital F-DS-898**

Como se visualiza en la anterior tabla, los riesgos asociados a los procesos se encuentran bajo la estructura del mapa de procesos con el cual inició operaciones la SDSCJ y como el nuevo mapa de riesgos de la Secretaría entró en vigencia a partir de septiembre de 2022 aprobado por el Comité de Gestión y Desempeño, esta Oficina de permite recomendar y reiterar la necesidad de actualizar la matriz de riesgos de seguridad digital, para así adicionar los procesos nuevos con sus activos de información y los riesgos de seguridad digital a los que haya lugar.

**4.1.4 Etapa 4: Valoración del riesgo:**

La valoración del riesgo, con base en lo mencionado en el informe del primer cuatrimestre, no presenta cambios debido a que no se ha actualizado la matriz de riesgos de seguridad digital. Con base en la versión 7 de la Política de Administración de riesgos institucional, para la valoración del riesgo, se debe calcular la probabilidad y el impacto de la siguiente manera:

**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° 2 Fuente Política De Administración Del Riesgo PO-DS-1 V7




**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° 3 Fuente Política De Administración Del Riesgo PO-DS-1 V7

Como se mencionó en el anterior informe de seguimiento, 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

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 se registran los controles diseñados para la administración de cada uno de los riesgos identificados, dichos controles, según la Matriz de riesgos de seguridad digital F-DS-898 V1. deben tener como mínimo la siguiente información:

INFORME DE SEGUIMIENTO A CONTROLES ASOCIADOS A LOS RIESGOS DE SEGURIDAD DIGITAL. II CUATRIMESTRE DE 2023

- Responsable (adecuado).
- Evidencias.
- Fuentes de información.
- Desviaciones u observaciones.
- Periodicidad.

Adicionalmente, respecto al objetivo del control tal como está definido en el numeral **10.7.1 de la política de administración de riesgos de la Entidad**, se presentan debilidades respecto a la estructura del control. A manera de ejemplo se mencionan los siguientes:

PROCESO	NOMBRE DEL CONTROL	COMENTARIO OCI
Acceso y Fortalecimiento de la Justicia	<p><u>Los responsable 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 repositorios SharePoint disponibles para el área.</u></p>	<p>Al contrastar el objetivo de este control con lo estipulado en la política de administración de riesgos, podría decirse que los verbos asociados son: entregan o solicitará. Por lo anterior, el objetivo del control no es claro frente a su acción.</p>
Gestión de Emergencias	<p><u>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 corresponde al Informe mensual de la empresa contratista. El cargue de las evidencias se hará trimestralmente.</u></p>	<p>Al igual que el caso anterior, el objetivo del control no es claro, puesto que el verbo usado es: delega.</p>

PROCESO	NOMBRE DEL CONTROL	COMENTARIO OCI
Gestión de Seguridad y Convivencia	<u>"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."</u>	El objetivo del control declara el verbo garantizar el cual se da por medio de un acta de proceso y custodia. Por lo mencionado el objetivo no tiene claridad de la acción a realizar.

Tabla N° 2 Elaboración propia. Fuente Matriz de riesgos de seguridad digital F-DS-898 V1.

Como se mencionó, lo anterior se sustenta de acuerdo con el numeral 10.7.1 de la política de administración de riesgos de la Entidad, el cual estipula lo siguiente:

o La definición debe incluir cuál es el Objetivo del control (valida, coteja, compara, concilia...)

Imagen N° 4 Fuente Política De Administración Del Riesgo PO-DS-1 V7

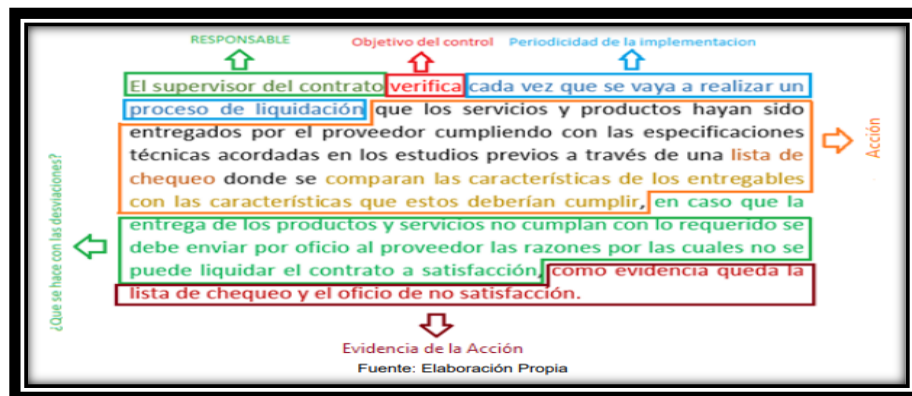


Imagen N° 5 Fuente Política De Administración Del Riesgo PO-DS-1 V7

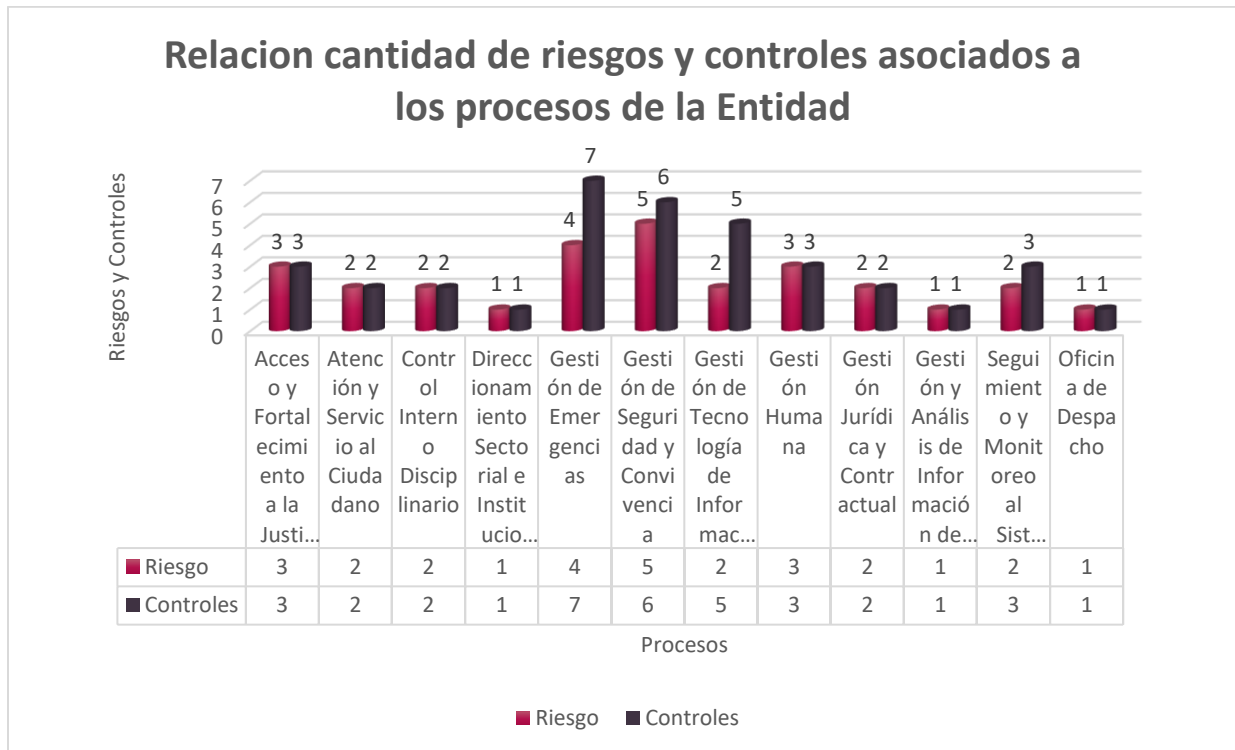
Con base en este sustento, se recomienda que la OAP y la DTSI trabajen de manera articulada para la actualización y alineación de los controles con la Política De Administración Del Riesgo PO-DS-1 V7 de la Entidad.

Ahora bien, respecto a los controles existentes, podemos mencionar que en referencia al primer cuatrimestre de la vigencia la cifra no varió, por tanto, nuevamente se reporta que para los **28** riesgos se ha identificado **36** controles

Proceso	Cantidad de controles identificados
Acceso y Fortalecimiento a la Justicia	3
Atención y Servicio al Ciudadano	2
Control Interno Disciplinario	2
Direccionamiento Sectorial e Institucional	1
Gestión de Emergencias	7
Gestión de Seguridad y Convivencia	6
Gestión de Tecnología de Información	5
Gestión Humana	3
Gestión Jurídica y Contractual	2
Gestión y Análisis de Información de S, C y AJ	1
Seguimiento y Monitoreo al Sistema de Control Interno	3
Oficina de Despacho	1
<b>TOTAL</b>	<b>36</b>

Tabla N° 3 Elaboración propia. Fuente Matriz de riesgos de seguridad digital F-DS-898 V1.

Con lo anterior y al realizar una equivalencia de los riesgos con sus controles identificados, presentamos la siguiente gráfica:



Gráfica N° 1 Elaboración propia. Fuente Matriz de riesgos de seguridad digital F-DS-898 V1.

**4.1.5.1 Evaluación de la estructura de controles:**

Frente a la estructura de controles, específicamente, se hacía énfasis en relación a los siguientes 4 procesos:

- ⊗ Acceso y Fortalecimiento de la Justicia,
- ⊗ Gestión Humana.
- ⊗ Gestión y Análisis de la Información de S,C y AJ.
- ⊗ Gestión de Seguridad y Convivencia.

Dado que, a la fecha de esta evaluación, no se observó rediseño en los controles, lo que a su vez genera reincidencia frente al anterior informe de seguimiento emitido por esta Oficina.

Lo anterior, permite evidenciar que no se ha realizado ninguna actividad de actualización a la matriz de riesgos de seguridad digital, continuando en versión número 1, para tal fin y con el ánimo reforzar el tema, una vez se haya recibido el presente informe de seguimiento, se recomienda generar un plan de acción con las actividades que se determinen a fin de atender la situación reportada.





A continuación, lo enunciado en el primer informe con radicado 3-2023-21506:

- ✚ **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 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.	No se describe claramente quien es el responsable de la ejecución del 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	Según el control esta tarea esta

N° Riesgo	N° Control	Proceso	Nombre de Control	Observación OCI
			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	asignada al equipo de nómina, por tanto, no tiene un responsable específico, tema que es ejecutado por la profesional especializada del área.

Tabla N°. 4. Elaboración Propia. Fuente: matriz de riesgos de seguridad digital F-DS-898

-  **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 portal 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.”*

#### 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. Esta situación se informó en el informe del primer cuatrimestre del año.

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

Como se mencionó en el informe del primer cuatrimestre, 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 riesgos.
- ✓ Responsable del proceso de verificación de los controles.
- ✓ Seguimiento de riesgos de manera cuatrimestral.

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

Como se ha mencionado a lo largo del presente documento, la matriz de riesgos de seguridad digital de la Entidad actualmente se compone de 28 riesgos con 36 controles asociados, cifras que continúan igual con lo reportado en el primer cuatrimestre.

Para el presente seguimiento correspondiente al segundo cuatrimestre de 2023, se evaluaron los controles obteniendo el siguiente resultado:

Código o Riesgo	Proceso	Control	Seguimiento OCI Primer cuatrimestre 2023	Recomendación I Cuatrimestre	Seguimiento y Recomendación OCI Segundo cuatrimestre 2023
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	Se evidencian 5 soportes donde se solicita por parte del profesional Universitario a los responsables, la información sobre metas de la dependencia.	No aplica	Se evidencian 2 soportes de electrónicos remitidos por la Dependencia responsable; el primero apunta a la solicitud de los reportes de seguimientos a metas por parte de un

INFORME DE SEGUIMIENTO A CONTROLES ASOCIADOS A LOS RIESGOS DE SEGURIDAD DIGITAL. II CUATRIMESTRE DE 2023

Código o Riesgo	Proceso	Control	Seguimiento OCI Primer cuatrimestre 2023	Recomendación I Cuatrimestre	Seguimiento y Recomendación OCI Segundo cuatrimestre 2023
		<p>tiempos establecidos, el Director de DAJ solicitara a los responsables la entrega oportuna de la información so pena del incumplimiento de metas, requerimientos internos y externos; como evidencia quedaran los soportes de la documentación entregada en los repositorios SharePoint disponibles para el área.</p>			<p>contratista y el segundo consiste en el reporte del contratista encargado a la Directora de la DAJ de los informes de casas de justicia mensuales y semestrales; de acuerdo con lo mencionado y al revisar la matriz de riesgos de seguridad digital, dentro de los activos catalogados se listan para la DAJ:</p> <p>(Plan de Acción de Casas de Justicia, Actas del Comité de Coordinación Local de las Casas de Justicia, Acciones Preventivo – Pedagógicas, Seguimiento a la Implementación del Traslado por Protección y Atención Psicológica a la Población Traslada, Historias de Procesos de Mediación para la Solución de Conflictos).</p> <p>Dicho lo anterior, 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.</p>

INFORME DE SEGUIMIENTO A CONTROLES ASOCIADOS A LOS RIESGOS DE SEGURIDAD DIGITAL. II CUATRIMESTRE DE 2023

Código o Riesgo	Proceso	Control	Seguimiento OCI Primer cuatrimestre 2023	Recomendación I Cuatrimestre	Seguimiento y Recomendación OCI Segundo cuatrimestre 2023
					Se recomienda generar soportes que apunten o cobijen todos los activos de información catalogados y en segunda instancia, es importante que la segunda línea de defensa intensifique los procesos de revisión y monitoreo de las evidencias a generar.
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.	Se evidencia correo electrónico remitido el día 28 de agosto del 2023 por parte de un contratista a la Directora de Acceso a la Justicia, en el cual se reportan las personas que tienen la administración de los formularios de la Dirección. De acuerdo con lo anterior, lo mencionado por la OCI en el seguimiento fue atendido por la dependencia responsable y el control se encuentra operando correctamente.
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	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	Actualizar el control de acuerdo con la realidad operativa del proceso, debido a que no se tiene un archivador para el depósito de documentos.	Se evidencia soporte de acta y correo generado respecto al manejo del archivador en el CER, lo cual refleja el cumplimiento del control. No obstante, lo anterior, en el informe

INFORME DE SEGUIMIENTO A CONTROLES ASOCIADOS A LOS RIESGOS DE SEGURIDAD DIGITAL. II CUATRIMESTRE DE 2023

Código o Riesgo	Proceso	Control	Seguimiento OCI Primer cuatrimestre 2023	Recomendación I Cuatrimestre	Seguimiento y Recomendación OCI Segundo cuatrimestre 2023
		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.	tanto, el control tal como está diseñado no se ejecuta.		de seguimiento del primer cuatrimestre se recomendó actualizar el control de acuerdo a la realidad operativa, puesto que se había informado la inexistencia del archivador en la dependencia, por ende la situación se reitera y se mantiene la misma recomendación.
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	Para este riesgo se observan las evidencias que soportan el control para el presente seguimiento. De acuerdo con el análisis realizado por el equipo de la OCI, se recomienda al encargado de la administración de riesgos de la OAP en conjunto con el Oficial de seguridad de la información, realizar un análisis frente al diseño y ejecución de este control y en caso de ser necesario actualizarlo.
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 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.	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 (esto para constatar la fecha de ejecución del control) y la comunicación complementaria en donde se solicite la	Complementar los soportes o evidencias de la ejecución del control de acuerdo con lo estipulado en el diseño.	Se evidencia reporte de usuarios activos e inactivos del sistema de información COPE, no obstante y al igual que en el anterior seguimiento, no se observan evidencias de la solicitud realizada a la DTSI sobre los usuarios del sistema, por lo anterior, la situación continua y por ende se sugiere a la OAP y a la DTSI realicen una revisión y análisis de

INFORME DE SEGUIMIENTO A CONTROLES ASOCIADOS A LOS RIESGOS DE SEGURIDAD DIGITAL. II CUATRIMESTRE DE 2023

Código o Riesgo	Proceso	Control	Seguimiento OCI Primer cuatrimestre 2023	Recomendación I Cuatrimestre	Seguimiento y Recomendación OCI Segundo cuatrimestre 2023
			activación o inactivación de usuarios.		este control para evaluar la efectividad y los soportes que se deben generar para certificar el cumplimiento de este.
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	Se observan correos electrónicos donde se autoriza el acceso a la información de la Oficina al Jefe, por lo cual el control está ejecutándose correctamente. De acuerdo con lo anterior, no se generan comentarios por parte de la OCI.
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 Disciplinarias 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	Se observan correos electrónicos donde se reportan quien tiene acceso a la información de la Oficina al Jefe, por lo cual el control está ejecutándose correctamente tal como se estimó. De acuerdo con lo anterior, no se generan comentarios por parte de la OCI.
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	Se evidencia soporte de ejecución del control tal como se estipula en el diseño.	No aplica	Para el presente seguimiento, se presentan evidencias de correos electrónicos remitidos por parte de la OAP a las dependencias, después de realizados los monitoreos a las publicaciones en el botón de transparencia. Por lo anterior el control

INFORME DE SEGUIMIENTO A CONTROLES ASOCIADOS A LOS RIESGOS DE SEGURIDAD DIGITAL. II CUATRIMESTRE DE 2023

Código o Riesgo	Proceso	Control	Seguimiento OCI Primer cuatrimestre 2023	Recomendación I Cuatrimestre	Seguimiento y Recomendación OCI Segundo cuatrimestre 2023
		evidencia quedara el correo de notificación y el esquema de publicación,			se encuentra operando en los términos definidos.
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 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	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, monitoreando los usuarios responsables que tienen acceso a los repositorios de información y realizando la respectiva depuración.	La dependencia reporta 7 soportes (uno mensual) de la ejecución del control, los cuales registran las solicitudes por de activación o creación de usuarios y permisos, por tanto la ejecución de control se encuentra operando correctamente.
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.	La Dirección de Talento Humano reporta evidencias mensuales de enero a junio con las planillas donde se registra el personal al cual se le realiza préstamo de historias laborales, por lo anterior, el control se está ejecutando correctamente.
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.	El control se está ejecutando correctamente de acuerdo con los soportes remitidos por parte de la Dependencia responsable.

INFORME DE SEGUIMIENTO A CONTROLES ASOCIADOS A LOS RIESGOS DE SEGURIDAD DIGITAL. II CUATRIMESTRE DE 2023

Código o Riesgo	Proceso	Control	Seguimiento OCI Primer cuatrimestre 2023	Recomendación I Cuatrimestre	Seguimiento y Recomendación OCI Segundo cuatrimestre 2023
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	Respecto a este control, la dependencia responsable remite el formato FUID de la vigencia 2023. De acuerdo con lo mencionado el control se está ejecutando correctamente.
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 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 en la vigencia 2023.	No aplica	Respecto a este control, la dependencia responsable remite el formato FUID de la vigencia 2023. De acuerdo con lo mencionado el control se está ejecutando correctamente.
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.	La dependencia responsable para el presente seguimiento remite los informes de interventoría número 53 y 55, con el informe de supervisión de contratos – formato 455.  De igual manera que en el seguimiento anterior, desde esta Oficina fue informado que el control contemplaba el reporte con las novedades, hallazgos y/o recomendaciones entregadas por parte del responsable del

INFORME DE SEGUIMIENTO A CONTROLES ASOCIADOS A LOS RIESGOS DE SEGURIDAD DIGITAL. II CUATRIMESTRE DE 2023

Código o Riesgo	Proceso	Control	Seguimiento OCI Primer cuatrimestre 2023	Recomendación I Cuatrimestre	Seguimiento y Recomendación OCI Segundo cuatrimestre 2023
					proyecto NUSE a la Jefatura del C4, por lo anterior la situación y al no presentar este soporte, el tema continua en la misma condición; por ende se recomienda a la OAP y la DTSI validar conjuntamente con el C4 respecto al cumplimiento del control y sus soportes o evidencias definidas. En caso de requerirse actualizar el control, es importante proceder de manera pronta.
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 novedades.	Se evidencian soportes de ejecución del control tal como este lo define. (Soportes de enero a abril de 2023)	No aplica	Se realiza revisión del soporte remitido por la dependencia responsable, informando que se está reportando evidencia del control (matriz) de los meses de agosto y septiembre, sin embargo, no se observan soportes correspondientes a los meses de mayo, junio y julio de la presente vigencia, por lo anterior, no se está cumpliendo el control generando la evidencia mensual tal y como se estipula. De acuerdo con lo informado, se recomienda que la OAP y la DTSI realicen un monitoreo y revisión puntual sobre este control en el C4, tomando las acciones necesarias para garantizar el cumplimiento cabal de

INFORME DE SEGUIMIENTO A CONTROLES ASOCIADOS A LOS RIESGOS DE SEGURIDAD DIGITAL. II CUATRIMESTRE DE 2023

Código o Riesgo	Proceso	Control	Seguimiento OCI Primer cuatrimestre 2023	Recomendación I Cuatrimestre	Seguimiento y Recomendación OCI Segundo cuatrimestre 2023
					lo definido en la matriz de riesgos de seguridad digital.
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 dejaron 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 como el control lo señala. De ser necesario evaluar la viabilidad de incluir en el control temas adicionales relacionados con seguridad de la información.	Basado en los soportes remitidos por el C4, el control se está cumplimiento dentro de los términos establecidos, no obstante, es importante complementar la evidencia con los “documentos de apoyo de las capacitaciones” que describe el control.
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	Una vez revisados los soportes remitidos por el C4 de la planta y la UPS, el control se está ejecutando dentro de los términos definidos.  Para este tema se recomienda reforzar los soportes entregados por parte de la dependencia responsable, puesto que para las UPS se remitieron evidencias de mayo y junio y para la planta, mayo, junio y julio.

INFORME DE SEGUIMIENTO A CONTROLES ASOCIADOS A LOS RIESGOS DE SEGURIDAD DIGITAL. II CUATRIMESTRE DE 2023

Código o Riesgo	Procesos	Control	Seguimiento OCI Primer cuatrimestre 2023	Recomendación I Cuatrimestre	Seguimiento y Recomendación OCI Segundo cuatrimestre 2023
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	El C4 remite carpetas correspondientes a los meses de mayo, junio y julio con las conciliaciones técnicas realizadas y derivadas del contrato de mantenimiento a las cámaras del sistema de video vigilancia, lo anterior se asocia a lo definido en el control. De acuerdo con lo informado, se sugiere que la OAP y DTSI, validen si los soportes actualmente remitidos como evidencia de ejecución, se asocian y cumplen lo descrito en el control, de lo contrario es importante actualizar la información del control en la matriz de riesgos de seguridad digital.
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. la 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: <i>“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”</i> ; por tanto y para soportar la ejecución del control,	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.	Se revisan los soportes remitidos por el C4 correspondientes a los meses de mayo y junio, en los cuales, dentro del informe mensual de contrato de mantenimiento del sistema de video vigilancia, se incluye el numeral 14.2 titulado incumplimientos de ANS con la penalización aplicada. Por lo sustentado anteriormente, el control se está ejecutando dentro de los parámetros establecidos.

INFORME DE SEGUIMIENTO A CONTROLES ASOCIADOS A LOS RIESGOS DE SEGURIDAD DIGITAL. II CUATRIMESTRE DE 2023

Código o Riesgo	Proceso	Control	Seguimiento OCI Primer cuatrimestre 2023	Recomendación I Cuatrimestre	Seguimiento y Recomendación OCI Segundo cuatrimestre 2023
			<p>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.</p>		
17	Gestión de Emergencias	<p>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. la Evidencia corresponde al Informe mensual de la empresa contratista. El cargue de las evidencias se hará trimestralmente.</p>	<p>Se evidencian soportes de ejecución del control tal como este lo define. (Soportes de Enero a marzo de 2023). Sin embargo, El control describe: <i>“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”</i>; 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.</p>	<p>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.</p>	<p>Se revisan los soportes remitidos por el C4 correspondientes a los meses de mayo y junio, en los cuales, dentro del informe mensual de contrato de mantenimiento del sistema de video vigilancia, se incluye el numeral 14.2 titulado incumplimientos de ANS con la penalización aplicada. Por lo sustentado anteriormente, el control se está ejecutando dentro de los parámetros establecidos.</p>

INFORME DE SEGUIMIENTO A CONTROLES ASOCIADOS A LOS RIESGOS DE SEGURIDAD DIGITAL. II CUATRIMESTRE DE 2023

Código o Riesgo	Proceso	Control	Seguimiento OCI Primer cuatrimestre 2023	Recomendación I Cuatrimestre	Seguimiento y Recomendación OCI Segundo cuatrimestre 2023
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 de proceso mediante correo electrónico y/o comunicado oficial.	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.	Se evidencia la ejecución del control el 21 de julio de 2023 con la revisión realizada a los usuarios del sistema de información progressus, cumpliendo con la frecuencia establecida. Sin embargo, y para fortalecer su ejecución, se recomienda a la dependencia responsable, generar la evidencia: <ul style="list-style-type: none"> <li>a. Solicitud a la DTSI el reporte de usuarios y roles.</li> <li>b. Correo electrónico enviado a líder del proceso evidenciando los funcionarios y contratista que tienen acceso.</li> <li>c. Informe al líder de proceso cuando se solicitan los retiros.</li> </ul>
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	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	Desarrollar y presentar el avance de la guía estipulada dentro del control para el siguiente cuatrimestre. Adicionalmente, se	La dependencia responsable remite guía borrador titulada "GUÍA FUNCIONAL PARA EL REGISTRO Y REVISIÓN DE ACTIVIDADES EN EL SISTEMA PROGRESSUS"

INFORME DE SEGUIMIENTO A CONTROLES ASOCIADOS A LOS RIESGOS DE SEGURIDAD DIGITAL. II CUATRIMESTRE DE 2023

Código o Riesgo	Proceso	Control	Seguimiento OCI Primer cuatrimestre 2023	Recomendación I Cuatrimestre	Seguimiento y Recomendación OCI Segundo cuatrimestre 2023
		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.	para el registro y verificación de la información.	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.	lo cual soporta el avance de la actividad.  Respecto a la segunda parte y al no haber validado el diseño del control para el presente seguimiento, se recomienda que la OAP y la DTSI en conjunto con la Subsecretaría de Seguridad y Convivencia, realicen revisión, ajuste y actualización de acuerdo con lo definido en la política de administración de riesgos de la Entidad.
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.	Se visualiza acta de reunión realizada el día 24 de julio del presente, donde se revisa y analiza el riesgo 19 con el control establecido; de acuerdo con lo anteriormente expuesto, el control se está ejecutando dentro de lo términos definidos, mencionando que la recomendación emitida por la OCI fue adoptada.
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 certificar el cumplimiento del	Se observan soportes correspondientes a los meses de mayo, junio, julio y agosto, es decir se está ejecutando el control con la frecuencia establecida. Lo anterior indica que la recomendación de la OCI fue acogida.

INFORME DE SEGUIMIENTO A CONTROLES ASOCIADOS A LOS RIESGOS DE SEGURIDAD DIGITAL. II CUATRIMESTRE DE 2023

Código o Riesgo	Proceso	Control	Seguimiento OCI Primer cuatrimestre 2023	Recomendación I Cuatrimestre	Seguimiento y Recomendación OCI Segundo cuatrimestre 2023
				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	Se observan soportes de la ejecución del control correspondientes al mes de mayo de 2023.  De acuerdo con la periodicidad establecida, no se adjuntan soportes de las actividades ejecutadas entre los meses de agosto y septiembre, por tanto, la OCI hace énfasis en el cumplimiento de lo descrito y estipulado en el control.
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	La dependencia responsable, remite archivos con registros y análisis estadísticos realizados, tal y como se estipula dentro del control.  Según lo validado por la OCI, en la parte final del control se describe que, en caso de no cumplir con el porcentaje establecido, se requerirá vía correo electrónico a los responsables; una vez validada la información estadística, se evidencian localidades con temas pendientes, por tanto, se debieron generar y adjuntar como evidencias complementarias de

INFORME DE SEGUIMIENTO A CONTROLES ASOCIADOS A LOS RIESGOS DE SEGURIDAD DIGITAL. II CUATRIMESTRE DE 2023

Código o Riesgo	Proceso	Control	Seguimiento OCI Primer cuatrimestre 2023	Recomendación I Cuatrimestre	Seguimiento y Recomendación OCI Segundo cuatrimestre 2023
					<p>este control los correspondientes correos.</p> <p>Expuesto lo anterior, se recomienda a la dependencia responsable reforzar la ejecución del control, tal como está definido, generando los soportes o evidencias que den fe de su cumplimiento, para tal fin, en el próximo seguimiento que ejecutará la OCI, se verificará este aspecto.</p>
23	Gestión de Tecnología de Información	<p>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</p>	<p>Se evidencia soporte de ejecución del control tal como este lo define.</p>	<p>No aplica</p>	<p>La DTSI remite una serie de documentos tales como actas de reunión, listados de asistencia, conceptos técnicos, entre otros, de los diferentes sistemas de información de la Entidad, no obstante, y en referencia al control específicamente, no se relacionan documentos tales como el soporte específico del seguimiento trimestral al cumplimiento del plan de actualización, plan de actualización y/o acta de aprobación. Lo anterior debería apuntar a la evidencia del control, la cual describe "reporte de seguimiento al plan o verificación del versionamiento en el ambiente de desarrollo y producción."</p>
23	Gestión de Tecnología	<p>El responsable de sistema de información realiza seguimiento trimestral a la ejecución del plan de</p>	<p>Se evidencia soporte de ejecución del control tal como este lo define. No</p>	<p>Adjuntar todos los manuales de los sistemas de</p>	<p>La evidencia compartida por la dependencia responsable consiste en</p>

INFORME DE SEGUIMIENTO A CONTROLES ASOCIADOS A LOS RIESGOS DE SEGURIDAD DIGITAL. II CUATRIMESTRE DE 2023

Código o Riesgo	Proceso	Control	Seguimiento OCI Primer cuatrimestre 2023	Recomendación I Cuatrimestre	Seguimiento y Recomendación OCI Segundo cuatrimestre 2023
	de Información	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.	obstante, solo se evidencia el manual del sistema de información SIGA.	información tal como está definido dentro del control, o en su defecto adjuntar el reporte de seguimiento al plan.	un documento de arquitectura de referencia de sistemas de información. En primera medida desde la OCI se menciona que dicho documento no tiene fecha de emisión, por lo cual, no se puede determinar el seguimiento trimestral o cuando fue generado; adicionalmente como segundo aspecto, el control define el plan de actualización documental, que tampoco no se relaciona dentro de los soportes y finalmente no se adjuntan los manuales técnicos de los sistemas de información, tal y como se recomendó en el informe de seguimiento del primer cuatrimestre de 2021 emitido por esta Oficina De acuerdo con lo mencionado, se recomienda que la OAP y DTSI realicen un proceso de inspección respecto a este control, determinado el detalle y los soportes que se deben generar.
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	Se evidencia soporte de ejecución del control tal como este lo define.	No aplica	La DTSI remite como evidencia el documento titulado “mecanismo para la gestión segura de credenciales de administración en la infraestructura tecnológica” con el cual se da cumplimiento a lo establecido en el control.

INFORME DE SEGUIMIENTO A CONTROLES ASOCIADOS A LOS RIESGOS DE SEGURIDAD DIGITAL. II CUATRIMESTRE DE 2023

Código o Riesgo	Proceso	Control	Seguimiento OCI Primer cuatrimestre 2023	Recomendación I Cuatrimestre	Seguimiento y Recomendación OCI Segundo cuatrimestre 2023
		alternativas adoptadas. Como evidencia de la ejecución del control se contará con el mecanismo de gestión segura de contraseñas o comunicado formal.			Para fortalecer lo anterior, se recomienda a la DTSI adicionar o incluir en el documento el seguimiento trimestral definido, por lo cual dicho documento debe tener una dinámica de actualización periódica.
24	Gestión de Tecnología de Información	El responsable de infraestructura define el plan de recuperación de información en sitio alternativo 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 alternativo 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 alternativo.	Generar el plan de recuperación de información en el sitio alternativo oficial de la Entidad, de acuerdo con lo definido en el control.	Respecto a este control, la DTSI remite 3 bitácoras de actividades y una priorización de servicios para continuidad; para este tema, desde la OCI se informa que las evidencias se asocian y están relacionadas con el control, sin embargo este no se ejecuta tal cual como está definido, puesto que no se remite plan de recuperación o comunicado oficial dirigido al Director de Tecnologías informando las alternativas adoptadas, por ende se recomienda realizar una revisión y monitoreo de este control por parte de la OAP y la DTSI, estableciendo acciones que garanticen su ejecución tal y como se tiene registrado, de lo contrario y si el caso lo amerita, ejecutar un proceso de actualización en la matriz de riesgos de seguridad digital.
24	Gestión de Tecnología	El responsable de infraestructura tecnológica realiza seguimiento trimestral al funcionamiento de	Se evidencian soportes de ejecución del control tal como este lo define.	No aplica	De acuerdo con las evidencias suministradas por la

INFORME DE SEGUIMIENTO A CONTROLES ASOCIADOS A LOS RIESGOS DE SEGURIDAD DIGITAL. II CUATRIMESTRE DE 2023

Código o Riesgo	Proceso	Control	Seguimiento OCI Primer cuatrimestre 2023	Recomendación I Cuatrimestre	Seguimiento y Recomendación OCI Segundo cuatrimestre 2023
	de Información	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.			DTSI, el control continúa ejecutándose correctamente, puesto que se relacionan 3 reportes del funcionamiento de la infraestructura de seguridad de la entidad.
25	Gestión y Análisis de Información de S, C y AJ	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.	Se evidencian soportes de ejecución del control tal como este lo define.	No aplica	La dependencia responsable remite 4 soportes con las fechas de actualización de la bodega de datos, con carácter mensual. No obstante, a lo anterior, y como el control lo describe, no se está adicionando a los soportes relacionados con el indicador de gestión, el cual permite determinar su cumplimiento, por tanto, se recomienda complementar los soportes para el siguiente informe de seguimiento por parte de esta Oficina, tema que debe ser validado previamente por la OAP y la DTSI.
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	Para el presente cuatrimestre, no se han generado solicitudes de acceso a información de usuarios a la carpeta de entes de control.

INFORME DE SEGUIMIENTO A CONTROLES ASOCIADOS A LOS RIESGOS DE SEGURIDAD DIGITAL. II CUATRIMESTRE DE 2023

Código o Riesgo	Proceso	Control	Seguimiento OCI Primer cuatrimestre 2023	Recomendación I Cuatrimestre	Seguimiento y Recomendación OCI Segundo cuatrimestre 2023
26	Seguimiento y Monitoreo al Sistema de Control Interno	La Jefatura de la Oficina de Control Interno al inicio de cada vigencia solicitará 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	Se evidencia el soporte presentado en el primer informe de seguimiento, por tanto, se da cumplimiento a lo definido en el control.
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	Se evidencian soportes de ejecución del control con fecha 14 de julio correspondiendo con la periodicidad definida, por lo tanto, el control continúa ejecutándose dentro de los términos establecidos.
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 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 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 claridad respecto al impacto del mismo dentro de la gestión de la Entidad.	El despacho remite soporte del correo remitido al Secretario informando la actualización de permisos para acceso a los documentos –actas.  En el seguimiento anterior, desde la OCI se menciona sobre la importancia de asociar este riesgo y control a un proceso oficial de la Entidad, situación que continua igual.  Adicionalmente y basado en la revisión del soporte remitido por el Despacho, se recomienda que sea

Código o Riesgo	Proceso	Control	Seguimiento OCI Primer cuatrimestre 2023	Recomendación I Cuatrimestre	Seguimiento y Recomendación OCI Segundo cuatrimestre 2023
					generado un espacio de asesoría por parte de la DTSI, frente al almacenamiento de archivos en One Drive asociado a un funcionario, y que no se esté utilizando las bibliotecas de información en SharePoint, situación que, en caso de rotación de personal, genera riesgos de disponibilidad de la información.

Tabla N°. 5. Elaboración Propia Fuente: Matriz de riesgos de seguridad digital F-DS-898 V1

Como resultado de lo anterior, se expone que, de los 36 controles definidos, se tienen comentarios y recomendaciones sobre 15 de estos es decir el 42 % en cuanto a la ejecución de estos (6% más que en el periodo anterior ya que se reportó un 36%).

En el presente seguimiento se reitera por parte de esta Oficina que **no todos los procesos tienen asociados controles de seguridad de la información** incluidos los nuevos, derivados de la actualización del mapa de procesos de la Secretaría, mencionando como por ejemplo los siguientes:

- ⊗ Gestión de Comunicaciones Estratégicas.
- ⊗ Gestión del conocimiento y la Innovación Pública
- ⊗ Fortalecimiento de Capacidades Operativas.
- ⊗ Gestión Financiera.
- ⊗ Gestión de Recursos Físicos al servicio de la Entidad.
- ⊗ Gestión Documental.
- ⊗ Gestión Integral a las personas privadas de la libertad – PPL.

#### 4.3. Seguimiento aspectos por mejorar identificados en el primer cuatrimestre de 2023:

*“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”.*

Ahora bien, para el presente seguimiento, se realizó validación de la anterior oportunidad de mejora con la Oficina Asesora de Planeación obteniendo como respuesta que *“actualmente se está cursando la actualización de la Política de Administración de Riesgos y dentro de los ajustes se tiene contemplado el ajuste de la periodicidad de evaluación de parte de la tercera línea de defensa, en el momento se tiene planteado de la siguiente forma:*

**“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	Tercera semana de mayo
Segunda corte: 31 de agosto	Tercera semana de octubre
Tercer corte: 31 de diciembre	Tercera semana de febrero

Tabla N° 6 Elaboración OAP. Fuente respuesta remitida por correo electrónico el día 20 de septiembre de 2023

De acuerdo con lo informado, esta situación se revisará en el siguiente informe de seguimiento con el fin de validar su estado.

## 5. CONCLUSIONES

- ✓ Los inventarios de activos de información de la Secretaría no se encuentran actualizados en concordancia al nuevo mapa de procesos, generando riesgos propios de seguridad de la información en pilares tales como confidencialidad, disponibilidad e integridad.
- ✓ Es importante que conjuntamente entre la OAP y la DTSI realicen revisión y monitoreo de los controles de seguridad digital en cuanto a su cumplimiento y generación de soporte o evidencias, apoyando a las dependencias en la correcta ejecución de estos, esto debido a que se generaron observaciones al 42% de los controles.
- ✓ Las evidencias que soportan la ejecución de controles se encuentran identificadas y organizadas por procesos, situación que permitió el análisis y ejecución del ejercicio auditor.

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