INFORME PRIMER CUATRIMESTRE RIESGOS DE SEGURIDAD DE LA INFORMACION - 2023

Dirección de Tecnologías y Sistemas de Información.

Mayo de 2023

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

Contenido

1. INTRODUCCIÓN

En cumplimiento a la Política de Administración de Riesgos de la Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ, específicamente en el ítem 15.3 “Seguimiento a la matriz de Seguridad digital F-DS-898”, el cual señala que *“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.*”, a continuación, se presentan los resultados evidenciados durante el primer cuatrimestre de la vigencia 2023.

El desarrollo de la matriz de riesgos de seguridad digital se basa en el trabajo previo de levantamiento de activos de información, realizado en la vigencia 2022 para los 18 procesos y 26 áreas de la Entidad, donde se validaron un total de 331 activos de información, los cuales fueron valorados por el personal de las áreas encargadas de acuerdo a los principios de Confidencialidad, Integridad y Disponibilidad de información, de los cuales 79 activos fueron clasificados con una valoración de criticidad Alta, 164 activos fueron clasificados con una valoración de criticidad Media y 88 activos fueron clasificados con una valoración de criticidad Baja.

Grafica 1. Elaboración propia

Sobre el ejercicio de levantamiento de riesgos de seguridad de la información| se tomaron como referencia los 79 activos de información clasificados con una valoración de criticidad Alta aprobados en las actividades previas de levantamiento de activos, de lo cual se validaron y

aprobaron mediante acta para toda la entidad un total de 28 riesgos y se generaron 36 controles estructurados de acuerdo a los parámetros establecidos en política de administración de riesgos de la Entidad para los procesos estratégicos, misionales, de apoyo y seguimiento y áreas, así:

ESTRATÉGICOS:

1. Direccionamiento Sectorial e Institucional (DS)
2. Gestión de Tecnología de Información (GT)

MISIONALES:

3. Gestión y Análisis de la Información de Seguridad, Convivencia y Acceso a la Justicia (GI)
4. Gestión de Seguridad y Convivencia (GS)
5. Acceso y Fortalecimiento a la Justicia (AJ)
6. Gestión de Emergencia (GE)

APOYO:

7. Atención y Servicio al Ciudadano (AS)
8. Gestión Jurídica y Contractual (JC)
9. Gestión Humana (GH)
10. Control Interno Disciplinario (CID)

SEGUIMIENTO:

11. Seguimiento y Monitoreo al Sistema de Control Interno (SM)

A su vez se contempla la información que gestiona la oficina del Despacho la cual se menciona de la siguiente forma:

OFICINA:

12. Oficina de Despacho (DES) (Sin Proceso)

La actualización de la Política de Administración de Riesgos a su Versión 7, realizada en al inicio del tercer trimestre de la vigencia 2022, da inicio a la validación del primer ejercicio sobre riesgos de seguridad de la información para la Entidad.

2. MATRIZ DE RIESGOS DE SEGURIDAD DIGITAL

Para el primer cuatrimestre del 2023, se dio gestión a la "Matriz de Riesgos de Seguridad Digital F-DS-898", la cual está disponible en la página WEB de la SDSCJ, en la siguiente ruta:

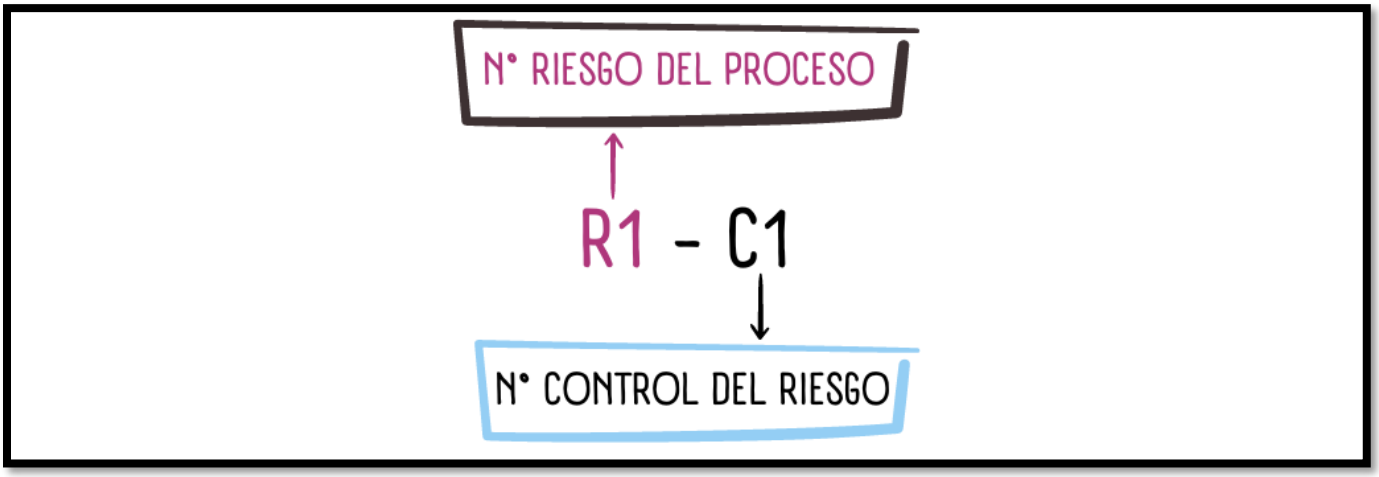
- **WEB**: https://scj.gov.co/es Transparencia y Acceso a la información pública - Planeación, políticas lineamientos y manuales - Matriz de riesgos seguridad digital – 2022.

  https://scj.gov.co/es/transparencia/planeacion/pol%C3%ADticas-lineamientos-y-manuales/matriz-riesgos-seguridad-digital-la

De manera general, todos los procesos poseen al menos un riesgo identificado y estos, a su vez, cumplen con lo establecido en la Política de Administración de Riesgos versión 7 adoptada por la SDSCJ, la cual obedece a los lineamientos otorgados por la "Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 - diciembre de 2020" del Departamento Administrativo de la Función Pública – DAFP.

Los siguientes son los lineamientos generales para la gestión de los Riesgos de seguridad de la información :

- Se cuenta con una (1) Matriz General de riesgos de seguridad digital con la agrupación de la información de los Riesgos de todos los procesos con la información de la Hoja de resumen, listado de activos, Riesgo Inherente, Tratamiento del Riesgo, Valoración con controles y Tratamiento de riesgo residual.
- Todos los Riesgos y controles cumplen con la metodología establecida en la Política de Administración de Riesgos versión 7.
- La nomenclatura de cada riesgo corresponde a razón de lo siguiente:



Grafica 2. Elaboración propia

Se informa que, durante el presente periodo no se recibieron notificaciones de ningún proceso con relación al ajuste de actividades control establecidas que impidieran la carga de las evidencias. A su vez no se recibió notificación respecto a la materialización de ningún riesgo.

La Dirección de Tecnologías y sistemas de información, en su mejora continua, realiza el primer ejercicio sobre la gestión de Riesgos de seguridad de la información y reitera su responsabilidad y compromiso en el apoyo metodológico requerido ante las posibles modificaciones o ajustes de las caracterizaciones, procedimientos y documentación que respalde la gestión de cada proceso y que conlleven al potencial cambio de riesgos o controles actualmente identificados. Se recuerda a cada proceso que es su responsabilidad mantener actualizada su documentación de acuerdo con la realidad operativa

La siguiente es la relación de la Matriz de Riesgos de Seguridad Digital, así:

# Riesgo	Proceso/Dependencia	Riesgo	Control
R1-C1	Acceso y Fortalecimiento a la Justicia	Pérdida de la Confidencialidad	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 repositorios SharePoint disponibles para el área.
R2-C1	Acceso y Fortalecimiento a la Justicia	Pérdida de la Integridad	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.

# Riesgo	Proceso/Dependencia	Riesgo	Control
R3-C1	Acceso y Fortalecimiento a la Justicia	Pérdida de la Disponibilidad Perdida de Confidencialidad	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 contará 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.
R4-C1	Atención y Servicio al Ciudadano	Pérdida de la Integridad Perdida de Confidencialidad	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.
R5-C1	Atención y Servicio al Ciudadano	Pérdida de la Integridad Perdida de Confidencialidad	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 él envió 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.
R6-C1	Control Interno Disciplinario	Pérdida de la Integridad	"El auxiliar administrativo de la oficina de Control Disciplinario interno designado, previa autorización del jefe OCDI, realiza cada vez que se requiera la autorización de acceso a los usuarios a la información, otorgando los permisos de lectura y/o edición de acuerdo 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.

# Riesgo	Proceso/Dependencia	Riesgo	Control
R7-C1	Control Interno Disciplinario	Pérdida de la Confidencialidad	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.
R8-C1	Direccionamiento Sectorial e Institucional	Pérdida de la Disponibilidad	El profesional asignado por la Oficina Asesora de Planeación para las publicaciones en el sitio web trimestralmente realiza el seguimiento y monitoreo a las publicaciones que se deben realizar por cada periodo en el sitio web de la Entidad mediante correo electrónico a los responsables con base al esquema de publicación. En caso de no recepcionar la información para publicación se deberá informar al Jefe de la Oficina de Planeación. Como evidencia quedara el correo de notificación y el esquema de publicación.
R9-C1	Gestión Humana	Pérdida de la Integridad	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
R10-C1	Gestión Humana	Pérdida de la Confidencialidad	La Dirección de Gestión Humana define el acceso de los usuarios autorizados y el equipo de archivo de la DGH, controlará el acceso al repositorio de historias laborales para la consulta y manejo de esta documentación, en caso de que los usuarios no cuenten con la autorización de acceso, no se permitirá la consulta a dichos expedientes, como evidencia se tendrá la base de préstamos de historias laborales. el cargue de evidencia se realizará Semestralmente
R11-C1	Gestión Humana	Pérdida de la Integridad	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

# Riesgo	Proceso/Dependencia	Riesgo	Control
R12-C1	Gestión Jurídica y Contractual	Pérdida de la Disponibilidad Perdida de la Confidencialidad Perdida de la Integridad	El responsable del equipo de archivo de la Dirección Jurídica y Contractual anualmente, realiza la intervención documental de los expedientes en referencia a la completitud y correspondencia de archivos de los expedientes que se maneja en el área, como evidencia se genera el inventario documental de la DJC. En caso de no entregar el inventario documental a las instancias correspondientes se debe informar al Director(a) Jurídico(a) y Contractual de las acciones para dar cumplimiento.
R13-C1	Gestión Jurídica y Contractual	Pérdida de la Disponibilidad Perdida de la Integridad	El responsable del equipo de archivo de la Dirección Jurídica y Contractual anualmente, realiza la intervención documental de los expedientes en referencia a la completitud y correspondencia de archivos de los expedientes que se maneja en el área, como evidencia se genera el inventario documental de la DJC. En caso de no entregar el inventario documental a las instancias correspondientes se debe informar al Director(a) Jurídico(a) y Contractual de las acciones para dar cumplimiento.
R14-C1	Gestión de Emergencias	Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad.	"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.
R14-C2	Gestión de Emergencias	Ausencia de personal	Grupo Operaciones C-4, mensualmente verifica la disponibilidad de personal asignado para el cumplimiento de las tareas dentro de la operación del NUSE123, de lo cual entregara una proyección sobre ausencia de personal y necesidades de operación. como evidencia se entregará matriz proyección de turnos operación de C4, para toma de decisiones. en caso de no contar con el personal necesario de operación envían un correo al jefe de C4, con las novedades.

# Riesgo	Proceso/Dependencia	Riesgo	Control
R14-C3	Gestión de Emergencias	Gestión deficiente de contraseñas	El grupo de entrenamiento C-4, semestralmente, realiza capacitación y /o sensibilización a funcionarios y contratistas sobre el correcto uso de contraseñas de acuerdo a lo establecido en el manual de seguridad y privacidad de la información de la Entidad, como soporte de la evidencia se dejarán las listas de asistencia y documentos de apoyo de las capacitaciones, para los casos que personal no asista se procede con la reprogramación de una nueva sesión de capacitación.
R15-C1	Gestión de Emergencias	Respuesta inadecuada de mantenimiento del servicio.	El grupo de seguimiento de infraestructura tecnológica del C-4, realizan la verificación de acciones preventivas y correctivas a UPS y Planta eléctrica programados en el contrato de mantenimiento establecido por parte de la Secretaría Distrital de Seguridad, convivencia y Justicia. Como evidencia se generan las actas del contratista del mantenimiento y los informes técnicos de funcionamiento de las UPS, en caso de no realizar los mantenimientos programados se deberá informar mediante correo electrónico sobre los motivos, así como las acciones para cumplir con los mantenimientos. el cargue de evidencia se hará trimestralmente.
R16-C1	Gestión de Emergencias	Trabajo no supervisado del personal externo o de limpieza.	El responsable del seguimiento del contrato de mantenimiento de video vigilancia, supervisa los mantenimientos externos a los equipos activos del sistema de video vigilancia, como evidencia se debe 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 entregará trimestralmente.
R16-C2	Gestión de Emergencias	Ausencia de acuerdos de nivel de servicio, o insuficiencia en los mismos.	El jefe del C4 delega a la empresa contratista el mantenimiento y operación del sistema de video vigilancia. Estas actividades se registran en informes de gestión de la empresa contratista recibidos de forma mensual evidenciando la operación del sistema de video vigilancia 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.

# Riesgo	Proceso/Dependencia	Riesgo	Control
R17-C1	Gestión de Emergencias	Uso incorrecto de software y hardware.	El jefe del C4 delega a la empresa contratista el mantenimiento y operación del sistema de comunicaciones. Estas actividades se registran en informes de gestión de la empresa contratista recibidos de forma mensual evidenciando la operación del sistema de comunicaciones controlada por ANS, que en caso de estar por debajo de umbral se penaliza económicamente. las Evidencia corresponde al Informe mensual de la empresa contratista. El cargue de las evidencias se hará trimestralmente.
R18-C1	Gestión de Seguridad y Convivencia	Pérdida de la Integridad y Disponibilidad	"El responsable de gestión de la información de Subsecretaría de seguridad y convivencia debe solicitar 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.
R18-C2	Gestión de Seguridad y Convivencia	Pérdida de la Integridad y Disponibilidad	"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.
R18-C2	Gestión de Seguridad y Convivencia	Pérdida de la Confidencialidad	"Él 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.

# Riesgo	Proceso/Dependencia	Riesgo	Control
R19-C1	Gestión de Seguridad y Convivencia	Pérdida de la Confidencialidad	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.
R20-C1	Gestión de Seguridad y Convivencia	Pérdida de la Confidencialidad	"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.
R21-C1	Gestión de Seguridad y Convivencia	Pérdida de la Integridad y Disponibilidad	"El responsable de gestión de la información de Subsecretaría de seguridad y convivencia 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.
R23-C1	Gestión de Tecnología de Información	Pérdida de la Integridad y Disponibilidad	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

# Riesgo	Proceso/Dependencia	Riesgo	Control
R23-C2	Gestión de Tecnología de Información	Pérdida de Confidencialidad, integridad y/o disponibilidad de la información	El responsable de sistema de información realiza seguimiento trimestral a la ejecución del plan de actualización documental de la arquitectura de los sistemas de información, en caso de no contar con el seguimiento trimestral al plan de actualización documental de la arquitectura, se deberá contar con los manuales técnicos actualizados de cada uno de los sistemas de información. Como evidencia de la ejecución del control se contará con el reporte de seguimiento al plan o con los manuales técnicos de los sistemas
R24-C1	Gestión de Tecnología de Información	Pérdida de Confidencialidad, integridad y/o disponibilidad de la información	El responsable de infraestructura define el mecanismo seguro y estandarizado para la gestión segura de credenciales de administración en la infraestructura tecnológica, así como el seguimiento trimestral al cumplimiento de los mecanismos establecidos, en caso de no contar con el seguimiento trimestral a los mecanismos establecidos, se contará con comunicación formal al Director de Tecnologías informando las alternativas adoptadas. Como evidencia de la ejecución del control se contará con el mecanismo de gestión segura de contraseñas o comunicado formal.
R24-C2	Gestión de Tecnología de Información	Pérdida de Confidencialidad, integridad y/o disponibilidad de la información	El responsable de infraestructura 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.
R24-C3	Gestión de Tecnología de Información	Pérdida de Confidencialidad, integridad y/o disponibilidad de la información	El responsable de infraestructura tecnológica realiza seguimiento trimestral al funcionamiento de herramientas de seguridad informática que protegen la información de la SDSCJ, en caso de no hacer seguimiento al funcionamiento se contara con comunicación formal al Director de Tecnologías informando las alternativas adoptadas. Como evidencia de la ejecución del control se contará con el reporte de rendimiento de la infraestructura de seguridad o el comunicado formal.

# Riesgo	Proceso/Dependencia	Riesgo	Control
R25-C1	Gestión y Análisis de Información de S, C y AJ	Pérdida de la Integridad	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.
R26-C1	Seguimiento y Monitoreo al Sistema de Control Interno	Pérdida de la Integridad	El profesional de la oficina de control interno designado, realiza cada vez que se requiera la autorización de acceso a los usuarios a la información, otorgando los permisos de lectura y/o edición de acuerdo al requerimiento, como soporte se contara con el correo electrónico, en caso de no contar con solicitud o requerimiento previo se debe solicitar la autorización a la jefatura de control interno, una vez sea autorizada, se debe dejar correo electrónico para efectos de trazabilidad.
R26-C2	Seguimiento y Monitoreo al Sistema de Control Interno	Pérdida de la Integridad	La Jefatura de la Oficina de Control Interno al inicio de cada vigencia solicitara a cada uno de los procesos y/o dependencias por escrito (Correo o Memorando), información de los enlaces responsables del diligenciamiento y reporte del avance del plan de mejoramiento institucional, en caso de no recibir respuesta del proceso y/o dependencias no se le autoriza acceso a la información. como evidencia se presentará el comunicado oficial enviado y las respuestas de los procesos y/o dependencias.
R27-C1	Seguimiento y Monitoreo al Sistema de Control Interno	Pérdida de la Integridad	El profesional de la Oficina de Control Interno de forma trimestral descarga el reporte del sistema de información en el que se genere el reporte a los planes de mejoramiento por procesos (internos) y se cargara este archivo en el repositorio SharePoint disponible para la Oficina de Control Interno. en caso de no poder descargar el reporte se solicitará a la DTSI se genere el reporte correspondiente por parte del administrador de la herramienta.

# Riesgo	Proceso/Dependencia	Riesgo	Control
R28-C1	Oficina del Despacho	Pérdida de la Integridad	El responsable de almacenamiento de las actas debe asegurar que los permisos otorgados a los usuarios sobre estos documentos, sean actualizados y/o retirados semestralmente, de acuerdo con los roles y permisos de cada funcionario que accede a la información, debe quedar como evidencia correo electrónico enviado a líder del proceso evidenciando los funcionarios que tienen acceso y el tipo de permiso que tienen (lectura, escritura, o ambos) En caso de que el responsable de almacenamiento de las actas no tenga permisos de gestión sobre la carpeta, deberá solicitarlos al secretario.

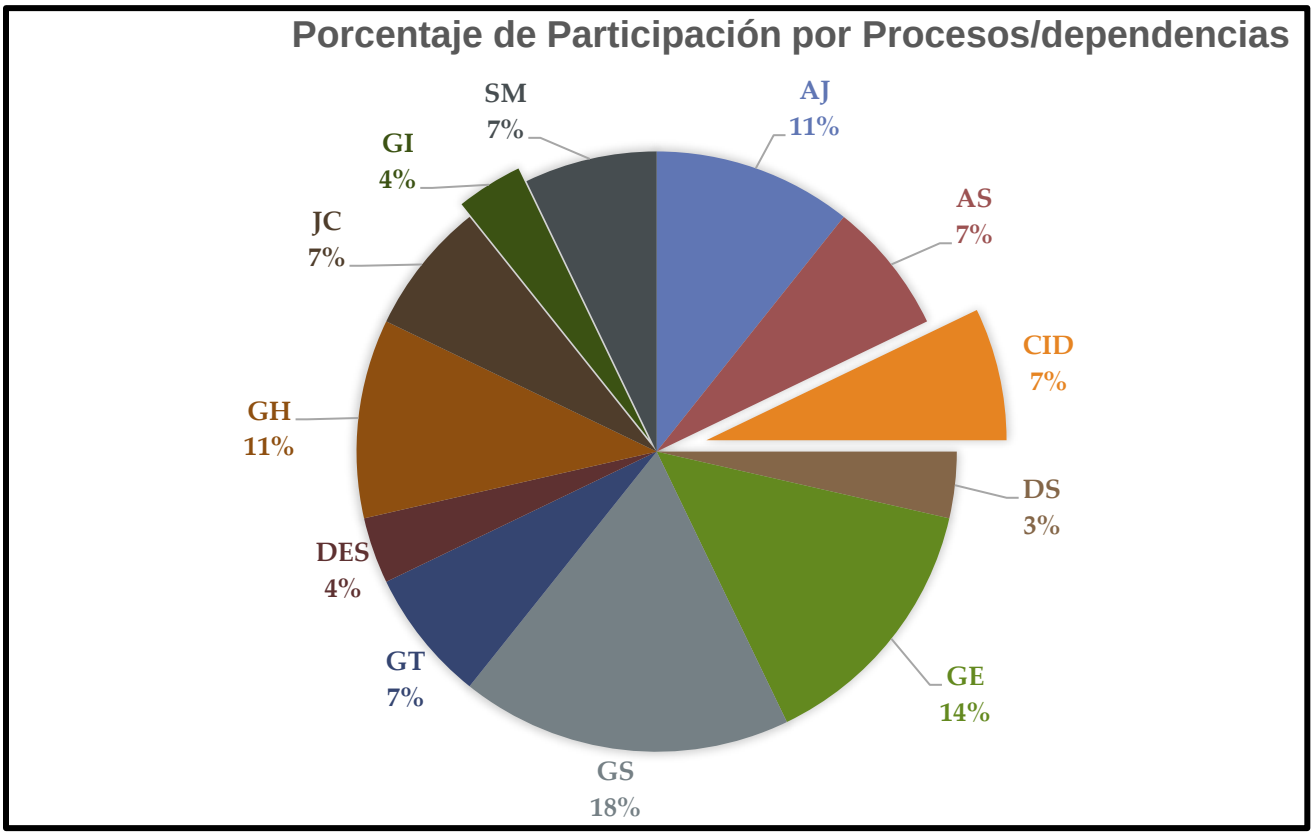
Tabla 1. Elaboración propia

3. ANALISIS DE LA MATRIZ DE RIESGOS

Los (28) veintiochos Riesgos de seguridad de la información se agrupan por Procesos/dependencia de la siguiente forma:

PROCESO/DEPENDENCIA	SIGLA	RIESGOS
Acceso y Fortalecimiento a la Justicia	**AJ**	**3**
Atención y Servicio al Ciudadano	**AS**	**2**
Control Interno Disciplinario	**CID**	**2**
Direccionamiento Sectorial e Institucional	**DS**	**1**
Gestión de Emergencias	**GE**	**4**
Gestión de Seguridad y Convivencia	**GS**	**5**
Gestión de Tecnología de Información	**GT**	**2**
Gestión Humana	**GH**	**3**
Gestión Jurídica y Contractual	**JC**	**2**
Gestión y Análisis de Información de S, C y AJ	**GI**	**1**
Seguimiento y Monitoreo al Sistema de Control Interno	**SM**	**2**
Oficina de Despacho	**DES**	**1**

Tabla 2. Elaboración propia



Grafica 3. Elaboración propia

Continuando con la gestión del riesgo se determina la valoración del riesgo, que se obtiene con la estimación de la probabilidad de ocurrencia e impacto a razón de los siguientes rangos:

Tabla Criterio de Probabilidad

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

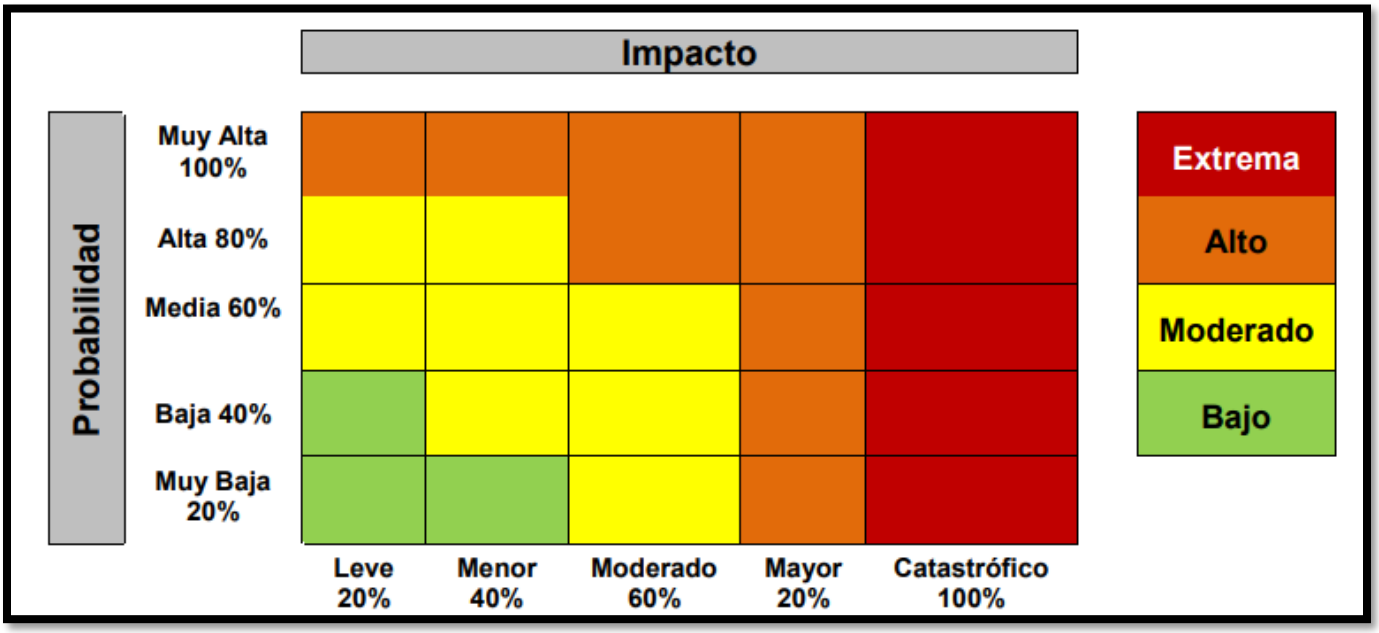
Grafica 4. Fuente: Política de Administración de Riesgos SDSCJ.

Tabla Criterio de impacto

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

Grafica 5. Fuente: Política de Administración de Riesgos SDSCJ.

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



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

Todas las valoraciones se realizaron de parte de los Líderes de proceso o los Líderes Operativos en compañía de sus grupos de trabajo, contando con el acompañamiento y orientación de la Dirección de Tecnologías y Sistemas de Información, dichas valoraciones de Probabilidad e Impacto nos dan como resultado la Zona de Riesgo Inherente resultado que se detalla en el siguiente cuadro.

PROCESO	EXTREMO	ALTO	MODERADO	BAJA	Total
Acceso y Fortalecimiento a la Justicia (AJ)			3		3
Atención y Servicio al Ciudadano (AS)			2		2
Control Interno Disciplinario (CID)			2		2
Direccionamiento Sectorial e Institucional (DS)		1			1
Gestión de Emergencias (GE)			4		4
Gestión de Seguridad y Convivencia (GS)			5		5
Gestión de Tecnología de Información (GT)		2			2
Gestión Humana (GH)			3		3
Gestión Jurídica y Contractual (JC)			2		2
Gestión y Análisis de Información de S, C y AJ (GI)		1			1
Seguimiento y Monitoreo al Sistema de Control Interno (SM)			2		2
Oficina de Despacho (DES).			1		1
Total	**0**	**4**	**24**	**0**	**28**

Tabla 3. Elaboración propia

Dada la necesidad de dar trámite y continuidad a los procedimientos y actividades establecidos por los procesos, para ninguno de los riesgos identificados se determinó “Evitar” como medida de tratamiento para el riesgo. Contrario a ello se optó por “Reducir el riesgo” como la medida por los procesos, con esto se hace necesaria la ejecución de controles para minimizar posibilidad de materialización de los riesgos, en concordancia con lo establecido en la Política de Administración de Riesgos de la Entidad.

Los siguientes son los riesgos y controles por proceso, aclarando que la cantidad de controles no está relacionada directamente con la materialización o no del riesgo. Los controles se han estructurado a consideración de cada proceso propendiendo evitar su posible materialización.

Proceso	N° Riesgos	N° Controles
Acceso y Fortalecimiento a la Justicia (AJ)	3	3
Atención y Servicio al Ciudadano (AS)	2	2
Control Interno Disciplinario (CID)	2	2
Direccionamiento Sectorial e Institucional (DS)	1	1
Gestión de Emergencias (GE)	4	7
Gestión de Seguridad y Convivencia (GS)	5	6
Gestión de Tecnología de Información (GT)	2	5
Gestión Humana (GH)	3	3
Gestión Jurídica y Contractual (JC)	2	2
Gestión y Análisis de Información de S, C y AJ (GI)	1	1
Seguimiento y Monitoreo al Sistema de Control Interno (SM)	2	3
Oficina de Despacho (DES).	1	1
Total	**28**	**36**

Tabla 4. Elaboración propia

Desde la Dirección de Tecnologías y Sistemas de Información se dio acompañamiento a todos los procesos para el cumplimiento de los anteriores parámetros permitiendo un cumplimiento global de todos los controles establecidos, lo que permite una apropiada gestión del riesgo.

El resultado de la gestión del riesgo con base en la ejecución de controles se puede apreciar a detalle en el siguiente cuadro comparativo de la Zona de Riesgo Inherente a la zona de Riesgo Residual:

PROCESO	INHERENTE					RESIDUAL				
	EXTREMO	ALTO	MODERADO	BAJA		EXTREMO	ALTO	MODERADO	BAJA
Acceso y Fortalecimiento a la Justicia (AJ)			3						3
Atención y Servicio al Ciudadano (AS)			2						2
Control Interno Disciplinario (CID)			2						2
Direccionamiento Sectorial e Institucional (DS)		1							1
Gestión de Emergencias (GE)			4						4
Gestión de Seguridad y Convivencia (GS)			5						5
Gestión de Tecnología de Información (GT)		2							2
Gestión Humana (GH)			3						3
Gestión Jurídica y Contractual (JC)			2						2
Gestión y Análisis de Información de S, C y AJ (GI)		1							1
Seguimiento y Monitoreo al Sistema de Control Interno (SM)			2						2
Oficina de Despacho (DES).			1						1
Total	**0**	**4**	**24**	**0**		**0**	**0**	**0**	**28**

Tabla 5. Elaboración propia

4. CARGUE EVIDENCIAS

La Política de Administración de Riesgos menciona la realización del seguimiento de la ejecución de los controles de seguridad de la información estructurados para todos los procesos de forma cuatrimestral. Para ello se puso a disposición de los líderes Operativos la Carpeta "*GobiernoTI/MIPG/Riesgos/SeguridadDigital*" en los repositorios SharePoint de la Entidad para el cargue de las evidencias correspondientes a la ejecución de los controles.

Mediante el siguiente enlace se puede acceder al repositorio SharePoint disponible para tal fin y verificar la información reportada, así:
https://scjgovcol.sharepoint.com/:f:/r/sites/DireccionTIC/Documentos%20compartidos/GobiernoTI/MIPG/Riesgos/Seguridad%20Digital/2023?csf=1&web=1&e=AvLA5o

La siguiente información se puede validar en dicha carpeta. Junto con los soportes compartidos para cada Riesgo por proceso:

Sigla	Proceso	N° Riesgos	N° Controles	Evidencias publicadas controles	% de riesgos cubierto
AJ	Acceso y Fortalecimiento a la Justicia	**3**	**3**	**3**	100%
AS	Atención y Servicio al Ciudadano	**2**	**2**	**7**	100%
CID	Control Interno Disciplinario	**2**	**2**	**2**	100%
DS	Direccionamiento Sectorial e Institucional	**1**	**1**	**3**	100%
GE	Gestión de Emergencias	**4**	**7**	**29**	100%
GS	Gestión de Seguridad y Convivencia	**5**	**6**	**6**	100%
GT	Gestión de Tecnología de Información	**2**	**5**	**5**	100%
GH	Gestión Humana	**3**	**3**	**3**	100%
JC	Gestión Jurídica y Contractual	**2**	**2**	**2**	100%
GI	Gestión y Análisis de Información de S, C y AJ	**1**	**1**	**5**	100%
SM	Seguimiento y Monitoreo al Sistema de Control Interno	**2**	**3**	**3**	100%
DES	Oficina del Despacho	**1**	**1**	**1**	100%
	Total	**28**	**36**	**69**	**100%**

Tabla 6. Elaboración propia

Lo anterior significa que los procesos cumplieron con la entrega de las evidencias de ejecución de los controles a la satisfacción basados los soportes suministrados.

De esta forma se confirma la sobresaliente gestión realizada en términos generales por los procesos que hacen parte de la Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ relacionado a la Administración y Gestión de los Riesgos de Seguridad de la Información.

La Dirección de Tecnologías y sistemas de Información se permite realizar las siguientes recomendaciones y/o comentarios con base a los controles establecidos y las evidencias suministradas:

# Riesgo	Proceso	Control	Recomendaciones
R9-C1	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 realizará Semestralmente	La periodicidad del control es semestral, mediante comunicado oficial se determina que las evidencias serán cargadas para el mes de mayo - junio en el segundo cuatrimestre, por lo cual se recomienda realizar las actividades correspondientes en los tiempos estimados.

# Riesgo	Proceso	Control	Recomendaciones
R10-C1	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 realizará Semestralmente	La periodicidad del control es semestral, mediante comunicado oficial se determina que las evidencias serán cargadas para el mes de mayo - junio en el segundo cuatrimestre, por lo cual se recomienda realizar las actividades correspondientes en los tiempos estimados.
R11-C1	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	La periodicidad del control es semestral, mediante comunicado oficial se determina que las evidencias serán cargadas para el mes de mayo - junio en el segundo cuatrimestre, por lo cual se recomienda realizar las actividades correspondientes en los tiempos estimados.
R28-C1	Oficina del Despacho	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.	La periodicidad del control es semestral, mediante comunicado oficial se determina que las evidencias serán cargadas para el mes de mayo - junio en el segundo cuatrimestre, por lo cual se recomienda realizar las actividades correspondientes en los tiempos estimados.

Tabla 7. Elaboración propia

5. CONCLUSIONES

En términos generales, finalizado el primer cuatrimestre del año 2023 la Dirección de Tecnologías y sistemas de información, ratifica su compromiso y participación realizando la revisión y seguimiento de la matriz de seguridad Digital, en cumplimiento a lo establecido en la Política de Administración de Riesgos y los Lineamientos establecidos por la "Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 - Diciembre de 2020" del DAFP contando con el soporte constante de los lideres Operativos de cada proceso.

Al realizar el seguimiento durante el primer cuatrimestre del 2023 a los Riesgos de seguridad de la información identificados por los procesos y oficinas enunciados, se puede concluir que la administración de los riesgos ha permitido la continuidad en la gestión, así como el logro de los objetivos definidos a los mismos, contribuyendo al fortalecimiento de la ejecución de actividades y blindando el cumplimiento de los objetivos de los procesos.

Es importante resaltar que la implementación efectiva de la Política de Administración de Riesgos está siendo liderada por la Dirección de Tecnologías y Sistemas de la Información para el caso de los Riesgos de Seguridad de la Información, con el apoyo de la Oficina Asesora de Planeación y el respaldo de la Oficina de Control Interno, ejercicio que es efectuado en cada proceso por los líderes operativos. Esto garantiza que la política se esté desarrollando y adoptando de manera adecuada durante el período actual en la Entidad.

Se pudo constatar el compromiso de los procesos en cumplir con la implementación de los controles establecidos en la matriz de seguridad digital al 100%. No se recibieron notificaciones de ningún proceso en cuanto a ajustes necesarios en las actividades de control que obstaculizaran la presentación de pruebas de cumplimiento. Además, no se reportaron situaciones en las que algún riesgo se haya materializado.

Se destaca el compromiso demostrado por los Líderes de Proceso y Líderes Operativos, así como por sus equipos de trabajo, al llevar a cabo de manera efectiva el desarrollo de los controles para los riesgos de seguridad de la información. Por este motivo, desde la Dirección de Tecnologías y Sistemas de Información, queremos expresar un reconocimiento merecido a todos los colaboradores que contribuyeron al logro de la meta de actualización durante el primer cuatrimestre del año 2023.

El levantamiento de activos de información para la vigencia 2023, establecido en la Política de Administración de Riesgos de la Entidad, se realiza de acuerdo a los cronogramas planeados para el nuevo organigrama de procesos, mediante mesas de trabajo por parte de personal de la Dirección de Tecnologías y Sistemas de Información, Dirección de recursos Físicos y Gestión Documental con el apoyo de la Oficina Asesora de Planeación.