ALCALDÍA MAYOR DE BOGOTÁ
SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA
AL RESPONDER CITAR EL NR.
Nro. Rad: 3-2024-2120
Fecha: 16/01/2024 02:23:07 PM
Destino: 130-OCI

MEMORANDO

Para: KAROL ANDREA PARRAGA HACHE
OFICINA DE CONTROL INTERNO

De: DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION

Asunto: INFORME TERCER CUATRIMESTRE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

Respetada Doctora: Parraga

En cumplimiento de la Política de Administración de Riesgos de la Secretaría Distrital de Seguridad, Convivencia y Justicia, así como siguiendo las directrices establecidas por el Departamento Administrativo de la Función Pública, se envía el informe cuatrimestral adjunto al presente documento sobre Riesgos de Seguridad de la Información. Este informe tiene como finalidad su revisión y socialización dentro de su área de responsabilidad.

Agradecemos de antemano sus consideraciones y comentarios al respecto.

Quedamos a su disposición para cualquier aclaración o consulta adicional.

Cordialmente,

IVAN HERSAYN PINILLA HERRERA
DIRECTOR DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION

c.c.e.: JORGE ELIECER VELASQUEZ PERILLA-DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION
RAFAEL HUMBERTO LOPEZ SAAVEDRA-DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION
EDWIN CASTILLO ORTIZ-DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION
FRANCISCO ALFORD BOJACA-COBRO PERSUASIVO
LUIS CARLOS GOMEZ CAMARGO-EQUIPO ATENCION AL CIUDADANO
CLAUDIA XIMENA HORMAZA LOZANO-EQUIPO ATENCION AL CIUDADANO
MARY LIZETH BUITRAGO SIERRA-OFICINA ASESORA DE PLANEACION
PABLO LEONARDO MOLANO PARRA-OFICINA ASESORA DE PLANEACION
JUAN DAVID GARCIA RUEDA-OFICINA ASESORA DE PLANEACION
KATHERINE BOLAGAY GAITAN-OFICINA DE CONTROL INTERNO
JOSE ALEXANDER PACHECO NORIEGA-OFICINA DE CONTROL DISCIPLINARIO INTERNO

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

JENNIFER CATHERINE VELASQUEZ-OFICINA DE CONTROL DISCIPLINARIO INTERNO
SAYRA GUINETTE ALDANA HERNANDEZ-OFICINA DE ANÁLISIS DE INFORMACION Y ESTUDIOS ESTRATEGICOS
DIANA MARCELA FLECHAS RUIZ-OFICINA DE ANÁLISIS DE INFORMACION Y ESTUDIOS ESTRATEGICOS
ADA LUZ SANDOVAL HERAZO-OFICINA CENTRO COMANDO, CONTROL, COMUNICACIONES Y COMPUTO C-4
EDITH NATHALIE ROMERO BARRERA-OFICINA CENTRO COMANDO, CONTROL, COMUNICACIONES Y COMPUTO C-4
ALEXANDER PALACIOS PALACIOS-OFICINA CENTRO COMANDO, CONTROL, COMUNICACIONES Y COMPUTO C-4
ANDRES CAMILO NIETO RAMIREZ-SUBSECRETARIA DE SEGURIDAD Y CONVIVENCIA
SANDRA MILENA PEREZ RAMIREZ-SUBSECRETARIA DE SEGURIDAD Y CONVIVENCIA
JULIANA CORTES GUERRA-SUBSECRETARIA DE ACCESO A LA JUSTICIA
VIVIANA PAOLA RODRIGUEZ RODRIGUEZ-SUBSECRETARIA DE ACCESO A LA JUSTICIA
MARCO ALEJANDRO GOMEZ ESLAVA-DIRECCION DE ACCESO A LA JUSTICIA
JORGE NICOLAS OLAYA MESA-DIRECCION DE ACCESO A LA JUSTICIA
SANDRA PATRICIA PINILLA MARTINEZ-DIRECCION DE GESTION HUMANA
ELIZABETH LESMES ARANDA-DIRECCION DE GESTION HUMANA
ANA MARIA MORENO GARCIA-DIRECCION JURIDICA Y CONTRACTUAL
MAGDA NATALY JAIMES RIVERA-DIRECCION JURIDICA Y CONTRACTUAL
ANDREA DEL PILAR ROJAS ALVAREZ-DESPACHO SECRETARIO DE SEGURIDAD
Anexos: 1

Elaboró: DIEGO MAURICIO USME GONZALEZ-DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION
Revisó: FABIO MIGUEL FONSECA REYES-DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION |
Aprobó: IVAN HERSAYN PINILLA HERRERA-DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION

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

INFORME TERCER CUATRIMESTRE RIESGOS DE SEGURIDAD DE LA INFORMACION - 2023

Dirección de Tecnologías y Sistemas de Información.

Enero de 2024

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 13. Publicación, Seguimiento y Evaluación a los Riesgos, se establece que la Segunda Línea de Defensa en este caso la Dirección de Tecnologías y Sistemas de la Información, "*Realiza cuatrimestralmente seguimiento a la Matriz de Riesgos y remitirá informe del resultado a la Oficina de Control Interno, los primeros 10 días hábiles, una vez vencido el cuatrimestre", se procede con la elaboración del presente informe representando lo identificado para el tercer cuatrimestre de la vigencia 2023.*".

El seguimiento a la matriz de riesgos de seguridad de información se basa en el trabajo previo de levantamiento de activos de información, donde se validaron un total de 331 activos de información, el personal responsable de cada proceso evaluó estos activos conforme a los principios de Confidencialidad, Integridad y Disponibilidad de información. De esta evaluación, se determinó que 79 activos fueron clasificados con una valoración de criticidad Alta, 164 activos con una valoración de criticidad Media y 88 activos con una valoración de criticidad Baja.

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, siendo aprobados en las actividades previas de levantamiento de activos, de lo cual se validaron y estructuraron mediante acta de reunión un total de 28 riesgos y se generaron 36 controles para toda la Entidad. Lo anterior de acuerdo con los parámetros establecidos en la Política de Administración de Riesgos de la Entidad, así:

ESTRATÉGICOS:

1. Atención y Relación con el Ciudadano. (AR)
2. Direccionamiento Estratégico (DE)
3. Fortalecimiento Institucional (FI)
4. Gestión de Tecnología de Información (GT).
5. Gestión y Análisis de la Información (GI).
6. Gestión Estratégica del Talento Humano (GH).

MISIONALES:

7. Acceso y Fortalecimiento a la Justicia (AJ)
8. Gestión de Emergencia (GE)
9. Gestión de Seguridad y Convivencia (GS)

APOYO:

10. Gestión Jurídica (GJ)

11. Gestión Contractual (GC)

SEGUIMIENTO:

12. Evaluación al Sistema de Control Interno (SM)
13. Control Interno Disciplinario (CID)

En términos generales, todos los procesos y áreas mencionadas han identificado al menos un riesgo, y estos cumplen con las pautas establecidas en la Política de Administración de Riesgos PO-FI-02 Ver. 1 adoptada por la SDSCJ. Dicha política está alineada con las directrices establecidas en la "Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 6 - noviembre de 2022" del Departamento Administrativo de la Función Pública – DAFP.

2. SOCIALIZACIÓN RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

En referencia a las actividades de socialización, por parte de la Dirección de Tecnologías y Sistemas de Información - DTSI, se realiza para el mes de diciembre, el diseño y presentación de pieza grafica sobre “Seguimiento a riesgos de seguridad de la información” mediante difusión masiva para toda la Entidad.

Gráfica.1 Elaboración Uso y Apropiación DTSI.

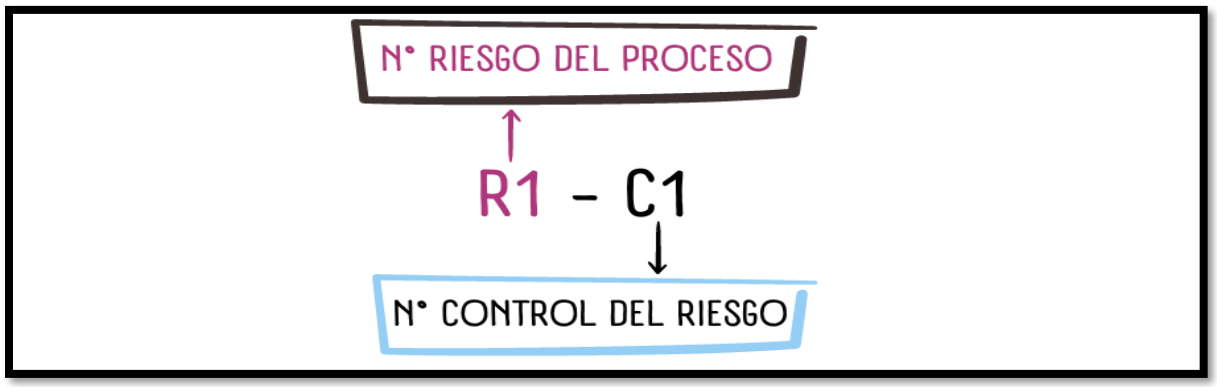
3. MATRIZ DE RIESGOS DE SEGURIDAD DE INFORMACIÓN

Para el tercer cuatrimestre del 2023, se dio gestión a la "Matriz de Riesgos de Seguridad de la información", 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 -Plan de acción - Matriz de riesgos seguridad de la Información – 2023.
  https://scj.gov.co/es/transparencia/planeacion-presupuesto-ingresos/plan-accion

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 de la información 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.
- La nomenclatura de cada riesgo corresponde a razón de lo siguiente:



Grafica 2. Elaboración propia

2.1. Cambios en la Matriz de Riesgos de Seguridad de la información.

La matriz de riesgos de seguridad digital F-DS-898 tuvo una migración propuesta de acuerdo con el modelo de operación por procesos en su versión 2, para lo cual tuvo una actualización al nuevo formato F-FI-1385 "Matriz de Riesgos de Seguridad de la información" en su versión 1, que está disponible en el Portal MIPG de la Entidad en el siguiente enlace:

https://portalmipg.scj.gov.co/lib/download.php?nivel1=a054VmZRbHVsejE2bHJsTHlMUUlEY3pIMDhCR0lBTkpFRDE5TmJWSFBaYVNjRTRKd1BvZ0Y5K0JwM2N1MDFMSU94emNyUGx4UlBlTkxmY1prVlNxNFE9PQ==&nivel2=QWh5Mmlua1BKU3hCTHlVRGFmSG9BKzZIRzBWU0NxelFvMXFsTWJPL2psST0=

2.2. Recomendaciones OCI.

En referencia a las conclusiones y recomendaciones generadas por la Oficina De Control Interno (OCI) mediante el radicado 3-2023-34057 “Informe de Seguimiento a Controles asociados a los Riesgos de Seguridad Digital”, emitido en el mes de septiembre de 2023, se realizaron mesas de trabajo con las áreas, para efectuar la validación de las observaciones emitidas por la Oficina de Control Interno sobre la evaluación de los controles presentados en el segundo cuatrimestre de la vigencia:

2.2.1. Proceso Acceso y Fortalecimiento a la Justicia (AJ).

- Recomendación riesgo 1 - control 1: Ajustar Control

Control Inicial:

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.

De acuerdo con las revisiones y análisis del control se propone por parte del grupo estructurador con el apoyo de la DTSI, los siguientes ajustes, así:

Control Ajustado:

Los responsables de la generación de información (funcionarios públicos y/o contratistas) verifican de forma cuatrimestral la entrega de soportes relacionados con el cumplimiento de metas relacionadas al Plan de Acceso a la Justicia de acuerdo con la naturaleza de los documentos (mensual - trimestral -semestral y anual) a la Dirección de Acceso a la Justicia. En caso de incumplimiento de la entrega de los documentos en los plazos establecidos, el Director o su equipo delegado de DAJ solicita a los responsables la entrega oportuna de la información, sopena del incumplimiento de metas, requerimientos internos y externos; como evidencia se entrega los soportes de la documentación entregada en los repositorios SharePoint disponibles para el área.

- Recomendación riesgo 2 – control 1: Ajustar Control

Control Inicial:

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.

De acuerdo con las revisiones y análisis del control se propone por parte del grupo estructurador con el apoyo de la DTSI, los siguientes ajustes, así:

Control Ajustado:

El profesional y/o los profesionales de la dirección de acceso designados para esta actividad trimestralmente solicita la verificación de los permisos de derecho de acceso a los diferentes formularios, de acuerdo con los roles y responsabilidades asignados para tal fin, como soporte de la revisión enviará este profesional comunicación oficial y/o correo electrónico a los responsables del área solicitando esta información, en caso que los usuarios no tengan autorización se retiraran permisos de acceso y se informara de las acciones al Jefe de área.

- Recomendación riesgo 3 - control 1: Ajustar Control.

Control Inicial:

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.

De acuerdo con las revisiones y análisis del control se propone por parte del grupo estructurador con el apoyo de la DTSI, la estructura del control:

Control Ajustado:

Los profesionales especializados encargados del área Jurídica y Atención Integral del CER, revisan cuatrimestralmente la información de la solicitud de autorización de acceso a la documentación archivada, este profesional tendrá a su cargo las llaves del archivador de documentos, contará con un documento oficial y/o correo electrónico de personas autorizadas al acceso de la información archivada; en caso de no contar con solicitud o requerimiento previo se debe solicitar esta autorización a la dirección del CER, una vez sea autorizada, se debe dejar este soporte para efectos de trazabilidad.

2.2.2. Proceso Atención y relación con el Ciudadano (AS).

- ❖ Recomendación riesgo 4 – control 1: Ajustar Control.

Control Inicial:

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.

De acuerdo con las revisiones y análisis del control se propone por parte del grupo estructurador con el apoyo de la DTSI y la Oficina asesora de Planeación, la estructura del control:

Control Ajustado:

El responsable del registro documental cuatrimestralmente realiza la verificación de la información recibida por parte de los reportes del sistema de gestión documental – SIGA, validando la integridad de la información y alimentando con esta el formato matriz de trazabilidad PQRS, como evidencia se entrega el formato diligenciado. En caso de que la información no este exacta y completa se deberá emitir correo electrónico y/o documento oficial a las partes interesadas solicitando las correcciones del caso.

- ❖ Recomendación riesgo 5 – control 1: Ajustar Control.

Control Inicial:

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.

De acuerdo con las revisiones y análisis del control se propone por parte del grupo estructurador con el apoyo de la DTSI y la Oficina asesora de Planeación, la estructura del control:

Control Ajustado:

El responsable del equipo de cobro persuasivo, semestralmente, verifica con el personal de soporte técnico los usuarios activos en el sistema de procesamiento de información de los expedientes de cobro persuasivo de acuerdo a los roles y responsabilidades asignados, como soporte de la revisión enviara correo electrónico y/o comunicación vía

Teams solicitando él envió de información y la respuesta requerida al personal encargado, en caso que exista usuarios no autorizados se solicita retirar los permisos de acceso e informar las actividades realizadas.

2.2.3. Proceso Gestión Estratégica del Talento Humano (GH).

- Recomendación riesgo 9 - control 1: Ajustar Control.

Control Inicial:

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.

De acuerdo con las revisiones y análisis del control se propone por parte del grupo estructurador con el apoyo de la DTSI, la estructura del control:

Control Ajustado:

El Profesional especializado responsable de nómina, solicita a la DTSI en caso de una novedad, el permiso y/o retiro de acceso de usuarios autorizados de forma permanente a los repositorios asignados para el manejo de esta información, como evidencia se tendrán las comunicaciones de solicitud y/o retiro de acceso de usuarios. En caso de que los permisos no sean gestionados correctamente se reitera la solicitud mediante correo electrónico a la mesa de servicio con los ajustes requeridos. El cargue de evidencia se realizará semestralmente.

2.2.4. Proceso de Gestión de Emergencias (GE).

- Recomendación riesgo 14 – control 1: Ajustar Control.

Control Inicial:

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.

De acuerdo con las revisiones y análisis del control se propone por parte del grupo estructurador de C-4, con apoyo de personal de la DTSI, los siguientes ajustes al control, así:

Control Ajustado:

El responsable del proyecto NUSE123, de forma mensual verifica los informes de seguimiento a la operación entregados por la empresa ETB y los informes de interventoría del cumplimiento aprobados para los tramites de pagos correspondientes. como evidencia se entregan los informes de seguimiento a la operación, informe de interventoría y el informe de supervisión, en caso de no contar con el reporte que entrega la empresa ETB y/o el informe de interventoría, se realizaran las gestiones pertinentes mediante comunicado oficial y/o correo electrónico sobre la solicitud de información.

- Recomendación riesgo 14 - control 2: Ajustar Control.

Para esta recomendación, se informa por parte del equipo de trabajo del proceso de Gestión de Emergencias (GE), que dentro de las evidencias presentadas se establece que en el próximo cumplimiento para el tercer cuatrimestre de riesgos de seguridad de Información se presentara de acuerdo con las recomendaciones de la OCI.

- Recomendación riesgo 16 - control 1: Ajustar Control.

Control Inicial:

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 entregará trimestralmente.

De acuerdo con las revisiones y análisis del control se propone por parte del grupo estructurador de C-4, con apoyo de personal de la DTSI, los siguientes ajustes al control, así:

Control Ajustado:

El responsable del seguimiento del contrato de mantenimiento de video vigilancia, supervisa los mantenimientos externos a los equipos activos del sistema de video vigilancia, como evidencia se debe presentar la conciliación técnica mensual provista por la empresa contratista y el responsable del seguimiento (Interventoría - supervisión SDSCJ), para los casos de mantenimiento en C-4 (instalaciones C-4 y DataCenter Bomberos) en caso de no contar con personal disponible de acompañamiento a la visita, no se autorizara el ingreso al personal externo y se reprogramara el mantenimiento. El cargue de las evidencias se hará de forma cuatrimestral.

- ❖ Recomendación riesgo 16 - control 2: Ajustar Control.

Control Inicial:

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.

De acuerdo con las revisiones y análisis del control se propone por parte del grupo estructurador de C-4, con apoyo de personal de la DTSI, los siguientes ajustes al control, así:

Control Ajustado:

El jefe del C4 supervisa a la empresa contratista del mantenimiento del sistema de video vigilancia y garantías extendidas del Centro de Computo. Estas actividades se registran en los informes de gestión de la empresa contratista, los cuales son recibidos y evidencian la operación del sistema de video vigilancia controlada por ANS, que en caso de estar por debajo de umbral se penaliza económicamente. Las Evidencias corresponde al Informe mensual de la empresa contratista e informe de seguimiento mensual del contrato. El cargue de las evidencias se hará de forma cuatrimestral.

2.2.5. Proceso Gestión de Seguridad y Convivencia (GS).

- ❖ Recomendación riesgo 18 – control 1: Ajustar Control.

Para esta recomendación, se informa por parte del equipo de trabajo del proceso Gestión de Seguridad y Convivencia (GS), dentro de las evidencias se entregó correo electrónico enviado a líder del proceso evidenciando los funcionarios y contratista que tienen acceso, Informe al líder de proceso cuando se solicitan los retiros.

Gráfica.3. Pantallazo Evidencia Control.

- Recomendación riesgo 18 – control 2: Ajustar Control.

Control inicial:

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 las revisiones y análisis del control se propone por parte del grupo estructurador con el apoyo de la DTSI, la estructura del control:

Control Ajustado:

El responsable de gestión de la información de la Subsecretaría de seguridad y convivencia, verifica la construcción y actualización de una guía para el uso adecuado de la plataforma que incluya lineamientos para el registro y verificación de la información; una vez construida la guía se actualizará cuatrimestralmente, como evidencia se contara con el correo electrónico a los líderes de equipo para su debida implementación, en caso de no realizar la actualización de la guía se contara con comunicación formal al líder del proceso.

- Recomendación riesgo 19 - control 1: Ajustar Control.

Control Inicial:

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.

De acuerdo con las revisiones y análisis del control se propone por parte del grupo estructurador con el apoyo de la DTSI, la estructura del control:

Control Ajustado:

"El(a) Director (a) de Seguridad, verifica en reunión cuatrimestral, que los documentos se almacenen en un sitio seguro dispuesto por la Entidad para restringir el acceso y uso únicamente para los usuarios autorizados, por medio de acta valida que el proceso de custodia y confidencialidad del documento final se realizó adecuadamente y/o de la aplicación de los correctivos necesarios, en caso de requerirse; en caso de no realizar la verificación se debe reprogramar dentro del mes posterior.

- Recomendación riesgo 21 - control 1: Ajustar Evidencias.

Para esta recomendación, se informa por parte del equipo de trabajo del proceso Gestión de Seguridad y Convivencia (GS), dentro de las evidencias se entregó en las evidencias del tercer cuatrimestre de riesgos de seguridad de Información (como se evidencia en la imagen siguiente) porque la periodicidad se estableció cada trimestre y esa evidencia correspondía al mes de septiembre del tercer trimestre, sin embargo, ya se hicieron los ajustes correspondientes.

Gráfica.4 Pantallazo Cargue Evidencia.

- Recomendación riesgo 22 - control 1: Ajustar Evidencias.

Para esta recomendación, se informa por parte del equipo de trabajo del proceso Gestión de Seguridad y Convivencia (GS), dentro de las evidencias presentadas se establece que en el próximo cumplimiento para el cuarto tercer cuatrimestre de riesgos de seguridad de Información se presentara de acuerdo con las recomendaciones de la OCI.

2.2.6. Proceso Gestión de Tecnología de Información (GT)

- Recomendación riesgo 23 - control 1: Ajustar Control.

Control Inicial:

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.

De acuerdo con las revisiones y análisis del control se propone por parte del grupo estructurador de la DTSI, los siguientes ajustes al control, así:

Control Ajustado:

El responsable de sistema de información y/o infraestructura Tecnológica verifica de forma cuatrimestral el seguimiento al plan de trabajo de versionamiento de los ambientes de pruebas y productivos asociados a los sistemas de información, en caso de no realizar

el seguimiento se debe evidenciar las causas de no realizar las actividades del plan a través de actas, informes y/o correos electrónicos, como evidencia de la ejecución del control se contara con los avances de las actividades del plan mediante bitácoras de actividades, actas y/o comunicado oficial.

- Recomendación riesgo 23 - control 2: Ajustar Control.

Control Inicial:

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.

De acuerdo con las revisiones y análisis del control se propone por parte del grupo estructurador de la DTSI, los siguientes ajustes al control, así:

Control Ajustado:

El responsable de sistema de información realiza seguimiento cuatrimestral a la ejecución del plan de actualización documental de la arquitectura de los sistemas de información, en caso de no contar con el seguimiento trimestral al plan de actualización documental de la arquitectura, se deberá contar con los manuales técnicos actualizados de cada uno de los sistemas de información. Como evidencia de la ejecución del control se contará con el reporte de seguimiento al plan o con los manuales técnicos de los sistemas.

- Recomendación riesgo 24 – control 2: Ajustar Control.

Control Inicial:

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.

De acuerdo con las revisiones y análisis del control se propone por parte del grupo estructurador de la DTSI, la estructura del control, así:

Control Ajustado:

El Líder o Coordinador de Infraestructura de TI de forma Anual o cada que se requiera es responsable de garantizar la disponibilidad de servicios internos de TI y reducir el riesgo de depender de un único proveedor de nube. Esto asegura la continuidad de las operaciones de la Entidad cuando hay cambios significativos en la infraestructura de TI o en la estrategia de proveedores de nube. Se verifica a través de desviaciones en el Plan de Contingencia de Servicios Tecnológicos y la Estrategia de Proveedores de Nube respaldados por la documentación correspondiente.

2.2.7. Proceso Gestión y Análisis de la Información (GI)

- Recomendación 1 - riesgo 25 - control 1: Ajustar Control.

Control Inicial:

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.

De acuerdo con las revisiones y análisis del control se propone por parte del grupo estructurador con el apoyo de la DTSI la estructura del control:

Control Ajustado:

El Profesional Universitario, Especializado y/o Contratista de la Oficina de Análisis de Información y Estudios Estratégicos responsable de la bodega de datos valida mensualmente que la carga de información de las fuentes haya finalizado exitosamente por medio de consultas SQL en el rango de fechas actualizado; cuyo resultado es evidenciado en el indicador de gestión "cumplimiento en la actualización de la bodega de datos" el cual es reportado periódicamente en el Portal MIPG. En caso de incumplimiento de este indicador se deberá realizar la justificación pertinente en el Portal MIPG. Como evidencias se adjunta la consulta SQL y el cargue en el portal MIPG del indicador de gestión asociado.

- Recomendación 2 - riesgo 25 - control 1.

Para esta recomendación, se informa por parte del equipo de trabajo del proceso Gestión y Análisis de la Información (GI), para la entrega de evidencias del tercer cuatrimestre (septiembre a diciembre) se solicitará al personal encargado del reporte de indicadores del proceso, el reporte de indicadores del Portal MIPG de los indicadores que se presentaron en la presente vigencia, para adjuntarlo en el cargue de evidencias.

Las mesas de trabajo llevadas a cabo por la Dirección de Tecnologías y Sistemas de la Información, en conjunto con las áreas pertinentes, fueron documentadas mediante la elaboración de las respectivas actas. Estas actas están disponibles para su consulta en los repositorios ubicados en la carpeta Share Point:

https://scjgovcol.sharepoint.com/:f:/r/sites/DireccionTIC/Documentos%20compartidos/Gobierno TI/MIPG/Riesgos/Seguridad%20Informaci%C3%B3n/Informes/2023/Segundo%20Cuatrimestre/Actas?csf=1&web=1&e=NnD3OO

2.3. Matriz de Riesgos de Seguridad de la Información.

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

# Riesgo	Proceso/Dependencia	Riesgo	Control
R1-C1	Acceso y Fortalecimiento a la Justicia	Pérdida de la Confidencialidad	Los responsables de la generación de información (funcionarios públicos y/o contratistas) verifican de forma cuatrimestral la entrega de soportes relacionados con el cumplimiento de metas relacionadas al Plan de Acceso a la Justicia de acuerdo con la naturaleza de los documentos (mensual - trimestral -semestral y anual) a la Dirección de Acceso a la Justicia. En caso de incumplimiento de la entrega de los documentos en los plazos establecidos, el Director o su equipo delegado de DAJ solicita a los responsables la entrega oportuna de la información, sopena del incumplimiento de metas, requerimientos internos y externos; como evidencia se entrega los soportes de la documentación entregada en los repositorios SharePoint disponibles para el área.
R2-C1	Acceso y Fortalecimiento a la Justicia	Pérdida de la Integridad	El profesional y/o los profesionales de la dirección de acceso designados para esta actividad trimestralmente solicita la verificación de los permisos de derecho de acceso a los diferentes formularios, de acuerdo con los roles y responsabilidades asignados para tal fin, como soporte de la revisión enviará este profesional comunicación oficial y/o correo electrónico a los responsables del área solicitando esta información, en caso que los usuarios no tengan autorización se retiraran permisos de acceso y se informara de las acciones al Jefe de área.

# Riesgo	Proceso/Dependencia	Riesgo	Control
R3-C1	Acceso y Fortalecimiento a la Justicia	Pérdida de la Disponibilidad Perdida de Confidencialidad	Los profesionales especializados encargados del área Jurídica y Atención Integral del CER, revisan cuatrimestralmente la información de la solicitud de autorización de acceso a la documentación archivada, este profesional tendrá a su cargo las llaves del archivador de documentos, contará con un documento oficial y/o correo electrónico de personas autorizadas al acceso de la información archivada; en caso de no contar con solicitud o requerimiento previo se debe solicitar esta autorización a la dirección del CER, una vez sea autorizada, se debe dejar este soporte para efectos de trazabilidad.
R4-C1	Atención y Relación con el Ciudadano.	Pérdida de la Integridad Perdida de Confidencialidad	El responsable del registro documental cuatrimestralmente realiza la verificación de la información recibida por parte de los reportes del sistema de gestión documental - SIGA, validando la integridad de la información y alimentando con esta el formato matriz de trazabilidad PQRS, como evidencia se entrega el formato diligenciado. En caso de que la información no este exacta y completa se deberá emitir correo electrónico y/o documento oficial a las partes interesadas solicitando las correcciones del caso.
R5-C1	Atención y Relación con el Ciudadano.	Pérdida de la Integridad Perdida de Confidencialidad	El responsable del equipo de cobro persuasivo, semestralmente, verifica con el personal de soporte técnico los usuarios activos en el sistema de procesamiento de información de los expedientes de cobro persuasivo de acuerdo a los roles y responsabilidades asignados, como soporte de la revisión enviara correo electrónico y/o comunicación vía Teams solicitando él envió de información y la respuesta requerida al personal encargado, en caso que exista usuarios no autorizados se solicita retirar los permisos de acceso e informar las actividades realizadas.
R6-C1	Control 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 con el 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.
R7-C1	Control 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.

# Riesgo	Proceso/Dependencia	Riesgo	Control
R8-C1	Fortalecimiento 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 Estratégica del Talento Humano.	Pérdida de la Integridad	El Profesional especializado responsable de nómina, solicita a la DTSI en caso de una novedad, el permiso y/o retiro de acceso de usuarios autorizados de forma permanente a los repositorios asignados para el manejo de esta información, como evidencia se tendrán las comunicaciones de solicitud y/o retiro de acceso de usuarios. en caso de que los permisos no sean gestionados correctamente se reitera la solicitud mediante correo electrónico a la mesa de servicio con los ajustes requeridos. El cargue de evidencia se realizará semestralmente.
R10-C1	Gestión Estratégica del Talento Humano.	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 Estratégica del Talento Humano.	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
R12-C1	Gestión Jurídica.	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.

# Riesgo	Proceso/Dependencia	Riesgo	Control
R13-C1	Gestión 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, de forma mensual verifica los informes de seguimiento a la operación entregados por la empresa ETB y los informes de interventoría del cumplimiento aprobados para los tramites de pagos correspondientes. como evidencia se entregan los informes de seguimiento a la operación, informe de interventoría y el informe de supervisión, en caso de no contar con el reporte que entrega la empresa ETB y/o el informe de interventoría, se realizaran las gestiones pertinentes mediante comunicado oficial y/o correo electrónico sobre la solicitud de información.
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.
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 con lo establecido en el manual de seguridad y privacidad de la información de la Entidad, como soporte de la evidencia se dejarán las listas de asistencia y documentos de apoyo de las capacitaciones, para los casos que personal no asista se procede con la reprogramación de una nueva sesión de capacitación.

# Riesgo	Proceso/Dependencia	Riesgo	Control
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 presentar la conciliación técnica mensual provista por la empresa contratista y el responsable del seguimiento (Interventoría - supervisión SDSCJ), para los casos de mantenimiento en C-4 (instalaciones C-4 y Data Center Bomberos) en caso de no contar con personal disponible de acompañamiento a la visita, no se autorizara el ingreso al personal externo y se reprogramara el mantenimiento. El cargue de las evidencias se hará de forma cuatrimestral.
R16-C2	Gestión de Emergencias	Ausencia de acuerdos de nivel de servicio, o insuficiencia en los mismos.	El jefe del C4 supervisa a la empresa contratista del mantenimiento del sistema de video vigilancia y garantías extendidas del Centro de Computo. Estas actividades se registran en los informes de gestión de la empresa contratista, los cuales son recibidos y evidencian la operación del sistema de video vigilancia controlada por ANS, que en caso de estar por debajo de umbral se penaliza económicamente. las Evidencias corresponde al Informe mensual de la empresa contratista e informe de seguimiento mensual del contrato. El cargue de las evidencias se hará de forma cuatrimestral.
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.

# Riesgo	Proceso/Dependencia	Riesgo	Control
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 la Subsecretaría de seguridad y convivencia, verifica la construcción y actualización de una guía para el uso adecuado de la plataforma que incluya lineamientos para el registro y verificación de la información; una vez construida la guía se actualizará cuatrimestralmente, como evidencia se contara con el correo electrónico a los líderes de equipo para su debida implementación, en caso de no realizar la actualización de la guía se contara con comunicación formal al líder del proceso.
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.
R19-C1	Gestión de Seguridad y Convivencia	Pérdida de la Confidencialidad	El(a) Director (a) de Seguridad, verifica en reunión Cuatrimestral, que los documentos se almacenen en un sitio seguro dispuesto por la Entidad para restringir el acceso y uso únicamente para los usuarios autorizados, por medio de acta valida que el proceso de custodia y confidencialidad del documento final se realizó adecuadamente y/o de la aplicación de los correctivos necesarios, en caso de requerirse; en caso de no realizar la verificación se debe reprogramar dentro del mes posterior.
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.

# Riesgo	Proceso/Dependencia	Riesgo	Control
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 y/o infraestructura Tecnológica verifica de forma cuatrimestral el seguimiento al plan de trabajo de versionamiento de los ambientes de pruebas y productivos asociados a los sistemas de información, en caso de no realizar el seguimiento se debe evidenciar las causas de no realizar las actividades del plan a través de actas, informes y/o correos electrónicos, como evidencia de la ejecución del control se contara con los avances de las actividades del plan mediante bitácoras de actividades, actas y/o comunicado oficial.
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 cuatrimestral a la ejecución del plan de actualización documental de la arquitectura de los sistemas de información, en caso de no contar con el seguimiento trimestral al plan de actualización documental de la arquitectura, se deberá contar con los manuales técnicos actualizados de cada uno de los sistemas de información. Como evidencia de la ejecución del control se contará con el reporte de seguimiento al plan o con los manuales técnicos de los sistemas
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 Líder o Coordinador de Infraestructura de TI de forma Anual o cada que se requiera es responsable de garantizar la disponibilidad de servicios internos de TI y reducir el riesgo de depender de un único proveedor de nube. Esto asegura la continuidad de las operaciones de la Entidad cuando hay cambios significativos en la infraestructura de TI o en la estrategia de proveedores de nube. Se verifica a través de desviaciones en el Plan de Contingencia de Servicios Tecnológicos y la Estrategia de Proveedores de Nube respaldados por la documentación correspondiente.

# Riesgo	Proceso/Dependencia	Riesgo	Control
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.
R25-C1	Gestión y Análisis de la Información.	Pérdida de la Integridad	El Profesional Universitario, Especializado y/o Contratista de la Oficina de Análisis de Información y Estudios Estratégicos responsable de la bodega de datos valida mensualmente que la carga de información de las fuentes haya finalizado exitosamente por medio de consultas SQL en el rango de fechas actualizado; cuyo resultado es evidenciado en el indicador de gestión "cumplimiento en la actualización de la bodega de datos" el cual es reportado periódicamente en el Portal MIPG. En caso de incumplimiento de este indicador se deberá realizar la justificación pertinente en el Portal MIPG. Como evidencias se adjunta la consulta SQL y el cargue en el portal MIPG del indicador de gestión asociado.
R26-C1	Evaluación 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	Evaluación 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	Evaluación 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	Direccionamiento Estratégico	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

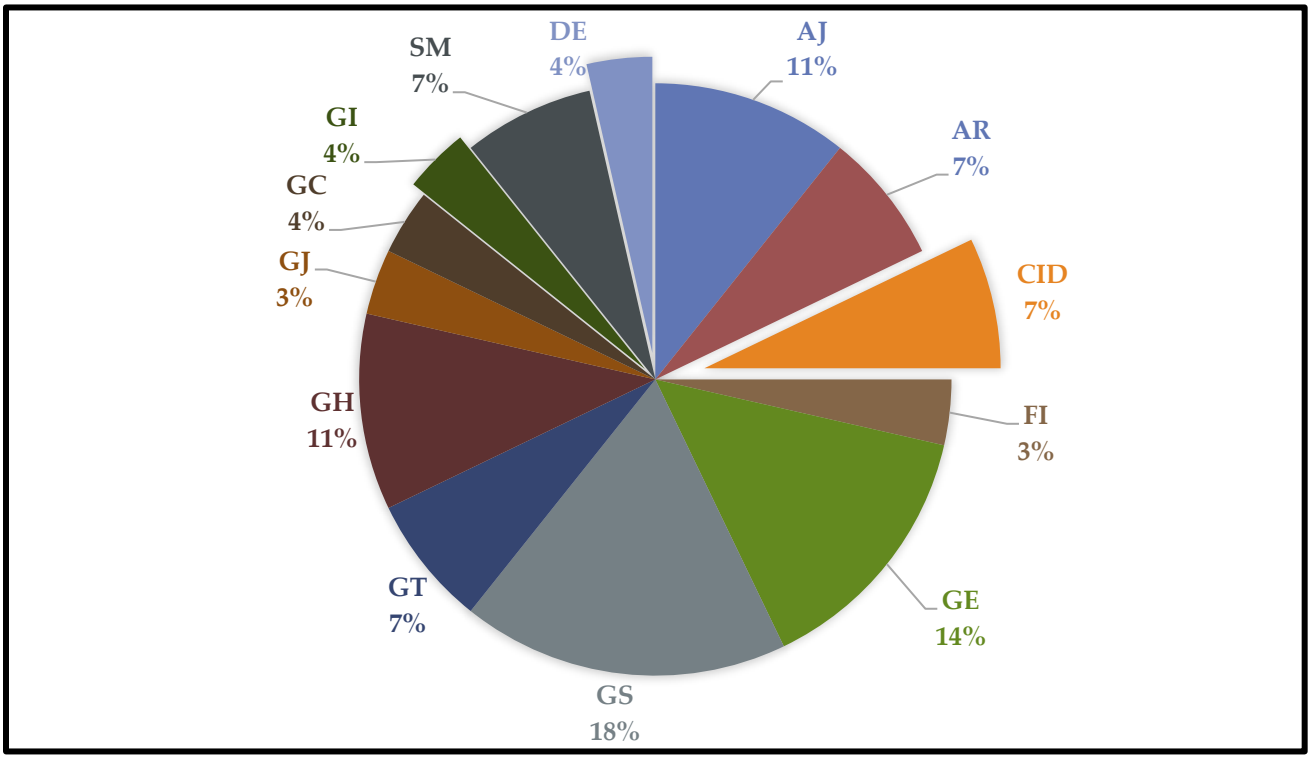
4. ANALISIS DE LA MATRIZ DE RIESGOS

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 Relación con el Ciudadano.	**AR**	**2**
Control interno Disciplinario.	**CID**	**2**
Fortalecimiento Institucional.	**FI**	**1**
Gestión de Emergencias	**GE**	**4**
Gestión de Seguridad y Convivencia	**GS**	**5**
Gestión de Tecnología de Información	**GT**	**2**
Gestión Estratégica del Talento Humano.	**GH**	**3**
Gestión Jurídica	**GJ**	**1**
Gestión Contractual	**GC**	**1**
Gestión y Análisis de Información	**GI**	**1**
Evaluación al Sistema de Control Interno.	**SM**	**2**
Direccionamiento Estratégico	**DE**	**1**

Tabla 2. Elaboración propia

Porcentaje de Participación por Procesos/dependencias



Grafica 5. 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%

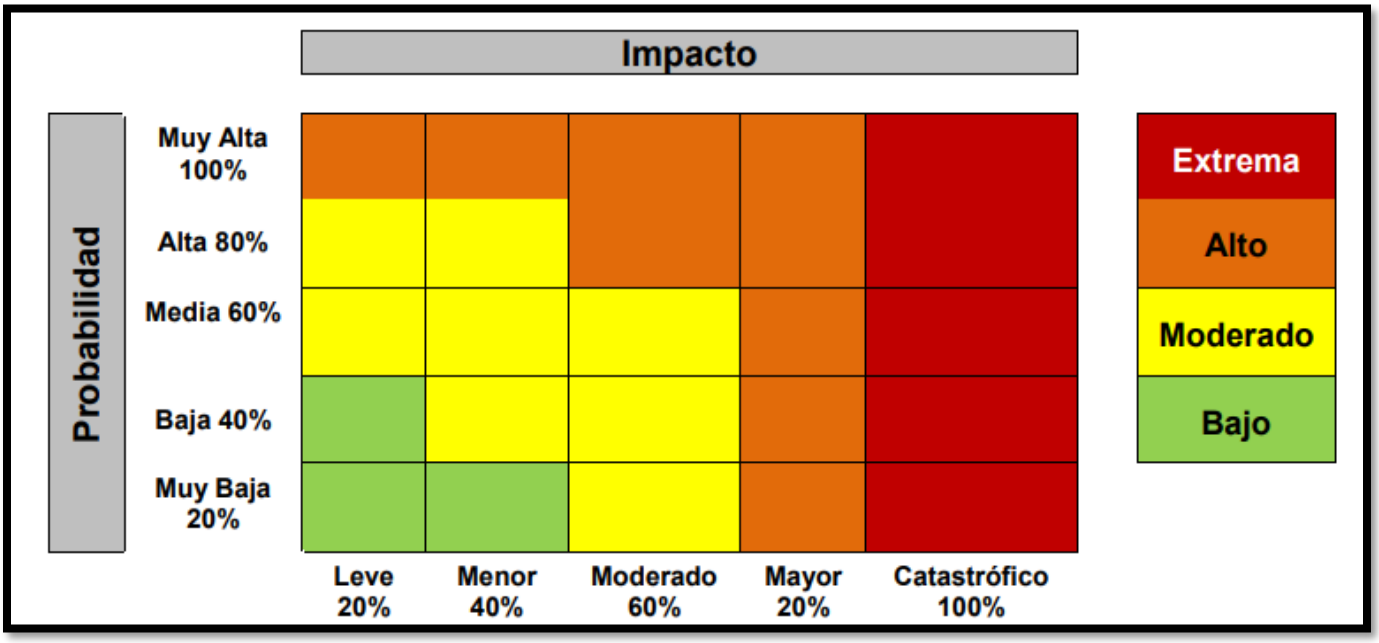
Grafica 6. Fuente: Política de Administración de Riesgos SDSCJ.

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 7. Fuente: Política de Administración de Riesgos SDSCJ.

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



Grafica 8. 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 Relación con el Ciudadano (AR)			2		2
Control Interno Disciplinario (CID)			2		2
Fortalecimiento Institucional (FI)		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 Estratégica del Talento Humano (GH)			3		3
Gestión Jurídica (GJ)			1		1
Gestión Contractual (GC)			1		1
Gestión y Análisis de Información (GI)		1			1
Evaluación al Sistema de Control Interno (SM)			2		2
Direccionamiento Estratégico (DE)			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.

La siguiente es la cantidad de 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 y sus recursos disponibles propendiendo evitar su posible materialización.

Proceso	N° Riesgos	N° Controles
Acceso y Fortalecimiento a la Justicia (AJ)	3	3
Atención y Relación con el Ciudadano (AR)	2	2
Control Interno Disciplinario (CID)	2	2
Fortalecimiento Institucional (FI)	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 Estratégica del Talento Humano (GH)	3	3
Gestión Jurídica (GJ)	1	1
Gestión Contractual (GC)	1	1

Proceso	N° Riesgos	N° Controles
Gestión y Análisis de Información de (GI)	1	1
Evaluación al Sistema de Control Interno (SM)	2	3
Direccionamiento Estratégico (DE)	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 Relación con el Ciudadano (AR)			2						2
Control Interno Disciplinario (CID)			2						2
Fortalecimiento Institucional (FI)		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 Estratégica del Talento Humano (GH)			3						3
Gestión Jurídica (GJ)			1						1
Gestión Contractual (GC)			1						1
Gestión y Análisis de Información de (GI)		1							1
Evaluación al Sistema de Control Interno (SM)			2						2
Direccionamiento Estratégico (DE)			1						1
Total	**0**	**4**	**24**	**0**		**0**	**0**	**0**	**28**

Tabla 5. Elaboración propia

5. CARGUE EVIDENCIAS

Mediante memorando interno 3-2023-44302 de fecha 12/12/2023 – DTSI, se realiza solicitud de cargue de información para el tercer cuatrimestre de la vigencia 2023, tomando como referencia la información generada en el informe de seguimiento a controles asociados a los riesgos de seguridad digital del segundo cuatrimestre de 2023 generado por la Oficina de Control Interno, donde se entrega información referente a los ajustes de entrega de evidencia por parte de los procesos y áreas para la presente vigencia.

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/SeguridadInformación*" 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%20Informaci%C3%B3n?csf=1&web=1&e=QNZB89

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%
AR	Atención y Relación con el Ciudadano	**2**	**2**	**2**	100%
CID	Control Interno Disciplinario	**2**	**2**	**1**	100%
FI	Fortalecimiento Institucional	**1**	**1**	**1**	100%
GC	Gestión Contractual	**1**	**1**	**1**	100%
GE	Gestión de Emergencias	**4**	**7**	**7**	100%
GH	Gestión Estratégica del Talento Humano	**3**	**3**	**3**	100%
GI	Gestión y Análisis de Información	**1**	**1**	**1**	100%
GJ	Gestión Jurídica	**1**	**1**	**1**	100%
GS	Gestión de Seguridad y Convivencia	**5**	**6**	**6**	100%
GT	Gestión de Tecnología de Información	**2**	**5**	**5**	100%
SM	Evaluación al Sistema de Control Interno	**2**	**3**	**3**	100%
DE	Direccionamiento Estratégico.	**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	Comentarios
R6-C1	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 con el 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.	No se presentó evidencias de control tomando como referencia que para el periodo no se requirió acceso de usuarios a información referente y la periodicidad de recolección es cada que se requiera, para lo cual se envió comunicado oficial.

Tabla 7. Elaboración propia

6. CONCLUSIONES

En términos generales, finalizado el tercer 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 de información, en cumplimiento a lo establecido en la Política de Administración de Riesgos y los Lineamientos establecidos por "Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 6 - noviembre de 2022" del Departamento Administrativo de la Función Pública – DAFP, contando con el soporte constante de los lideres Operativos de cada proceso.

Al realizar el seguimiento durante el tercer 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.

Tras llevar a cabo mesas de trabajo con las áreas definidas, en respuesta al informe de seguimiento de la Oficina de Control Interno (OCI) con el radicado 3-2023-34057, referente a los controles asociados a los riesgos de seguridad digital emitido en septiembre de 2023, se avanzó significativamente en la validación de las observaciones realizadas por la OCI, que ha permitido una evaluación de los controles presentados. Al igual, se valora el compromiso y la colaboración de todas las áreas involucradas en estas actividades, para la implementación de las mejoras recomendadas para la efectividad de los controles.

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 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.

Para el levantamiento de activos de información para la vigencia 2023, establecido en la Política de Administración de Riesgos de la Entidad, se elaboró un cronograma para adelantar esta actividad en el II semestre 2023, sin embargo dada la contingencia de la actualización del mapa

de procesos, se propone para la publicación en Datos Abiertos y se evite el reproceso de esta recolección de información, la publicación del Registro de Activos de Información e Índice de Información Clasificada y Reservada con la información de la vigencia 2022, de acuerdo a las mesas de trabajo integradas entre la Oficina Asesora de Planeación, Dirección de Recursos Físicos y gestión Documental y La Dirección de Tecnologías y Sistemas de Información.

La Dirección de Tecnologías y sistemas de información, en su mejora continua, para el ejercicio sobre la gestión de Riesgos de seguridad para la vigencia 2023 de la información, 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