Unidad para las Víctimas

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2026

Oficina de Tecnologías de la Información

Unidad para las Víctimas

TABLA DE CONTENIDO

Imágenes

Tablas

Unidad para las Víctimas

1. Introducción

El aseguramiento de la Información en términos de confidencialidad, integridad y disponibilidad hace parte esencial para la adecuada operación misional de la Entidad, contemplando todos los procesos estratégicos, misionales, de apoyo y de seguimiento y control. En este sentido, es crucial identificar y tratar los riesgos de seguridad de la información asociados a los activos de información críticos, toda vez que, en el escenario de la materialización de incidentes de seguridad, se pueden generar consecuencias e impactos significativos no solo en términos económicos, sino también en la reputación y continuidad operativa de la entidad.

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información tiene como objetivo principal definir y priorizar las medidas necesarias para mitigar estos riesgos, asegurando así la continuidad de las operaciones y la protección de los datos sensibles. Para ello, se establecen controles y planes de tratamiento específicos destinados a gestionar eficazmente los riesgos identificados.

Además, el plan contempla la asignación de responsables y recursos necesarios para implementar y mantener estas medidas de manera efectiva, promoviendo una cultura de seguridad en toda la entidad. Este enfoque integral garantiza que todos los miembros de la organización estén comprometidos con la seguridad de la información y contribuyan activamente a la protección de los activos críticos.

2. Objetivo General

Definir y priorizar las medidas necesarias para mitigar estos riesgos, asegurando así la continuidad de las operaciones y la protección de los datos sensibles de la **Unidad para las Victimas**.

3.1. Objetivo Específico

- Identificar, evaluar y mitigar los riesgos asociados a los activos de información críticos con el fin de preservar la Confidencialidad, Integridad y Disponibilidad de la información.

- Definir e implementar controles de seguridad que mitiguen los riesgos identificados en cada uno de los procesos de la Entidad.

3. Alcance

Este plan tiene como finalidad la consolidación de los controles y planes de tratamiento de los riesgos de seguridad de la información identificados en el marco de la metodología establecida por la Entidad para tal fin. Esta consolidación permitirá realizar seguimiento a la ejecución de las actividades establecidas con el propósito de fortalecer la confidencialidad, integridad y disponibilidad de la información administrada por los procesos de la Unidad para la Atención y Reparación Integral de las Víctimas.

4. Definiciones.

- **Activos de Información[1]:** Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas) que tenga valor para la organización.

- **Amenaza[2]:** (Inglés: Threat). Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

- **Confidencialidad[3]:** (Inglés: Confidentiality). Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

- **Control[4]:** medida que mantiene y/o modifica un riesgo.

  Nota: Los controles incluyen, pero no se limitan a cualquier proceso, política, dispositivo, práctica u otras condiciones y/o acciones que mantengan y/o modifiquen un riesgo.

- **Disponibilidad[5]:** (Inglés: Availability). Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

- **Integridad[6]:** (Inglés: Integrity). Propiedad de la información relativa a su exactitud y completitud.

- **Impacto[7]:** (Inglés: Impact). El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

[1] Fuente de definición: https://www.iso27000.es/glosario.html.
[2] Fuente de definición: https://www.iso27000.es/glosario.html.
[3] Fuente de definición: https://www.iso27000.es/glosario.html.
[4] Fuente de definición: ISO 31000:2018.
[5] Fuente de definición: https://www.iso27000.es/glosario.html.
[6] Fuente de definición: https://www.iso27000.es/glosario.html.
[7] Fuente de definición: https://www.iso27000.es/glosario.html.

- **Riesgo[8]:** (Inglés: Risk). Efecto de la incertidumbre sobre los objetivos.

- **Tratamiento de Riesgo[9]:** El propósito del tratamiento de los riesgos es seleccionar e implementar opciones para abordar los riesgos. El tratamiento de los riesgos implica un proceso iterativo de:

  a. Formular y seleccionar opciones para el tratamiento de los riesgos.
  b. Planear e implementar el tratamiento de los riesgos.
  c. Evaluar la efectividad de dicho tratamiento.
  d. Decidir si los riesgos residuales son aceptables.
  e. Si no son aceptables, efectuar algún tratamiento adicional.

- **Vulnerabilidad[10]:** (Inglés: Vulnerability). Debilidad de un activo o control que puede ser explotada por una o más amenazas.

5. Marco de Referencia

La **Unidad para las Víctimas** toma como marco de referencia para la gestión de Riesgos las normas y estándares internacionales como:

- NTC-ISO/IEC 31000.
- NTC-ISO/IEC 27005.
- NTC-ISO/IEC 27001.

6. Metodología

Se aplican los lineamientos definidos en la Metodología de Administración de Riesgos de la Entidad, esta puede ser consultada en el link: https://www.unidadvictimas.gov.co/NODE/45506.

[8] Fuente de definición: https://www.iso27000.es/glosario.html.
[9] Fuente de definición: ISO 31000:2018.
[10] Fuente de definición: https://www.iso27000.es/glosario.html.

7. Planes de Tratamiento al Riesgo

La definición y ejecución del Plan de Tratamiento de Riesgos de Seguridad de la Información es fundamental para garantizar la seguridad y protección de los activos de información de la **Unidad para las Víctimas**. Este plan permite identificar, evaluar y gestionar los riesgos que puedan comprometer la confidencialidad, integridad y disponibilidad de la información.

La ejecución del Plan de Tratamiento de Riesgos fortalece la capacidad de la Entidad para enfrentar posibles amenazas y busca generar un entorno de operación seguro. Este enfoque está alineado con los estándares de seguridad y cumplimiento normativo, lo que contribuye a la resiliencia y confianza en los procesos de la Entidad. A continuación, se relaciona la cantidad de riesgos, controles y planes identificados para la Entidad.

Proceso	Riesgos	Controles	Plan Acción
Reparación Integral	1	3	1
Direccionamiento Estratégico	1	2	2
Gestión de Talento Humano	1	2	1
Registro y Valoración	1	4	1
Gestión Documental	1	3	2
Gestión Financiera	2	4	3
Gestión Administrativa	2	6	1
Gestión Contractual	2	4	2
Gestión Jurídica	2	4	2
Control Interno Disciplinario	2	3	1
Evaluación Independiente	2	3	0
Relación con el Ciudadano	1	3	3
Gestión Interinstitucional	1	3	1
Prevención Urgente Atención Inmediatez	1	3	1
Gestión para la Asistencia	1	1	2
Participación y Visibilización	1	3	1
Gestión de Información	10	30	12
Total	**32**	**81**	**36**

Tabla No.1 - Riesgos, Controles y Planes de Seguridad.

Los 32 riesgos identificados en los procesos de nivel nacional tienen el siguiente nivel de riesgo residual

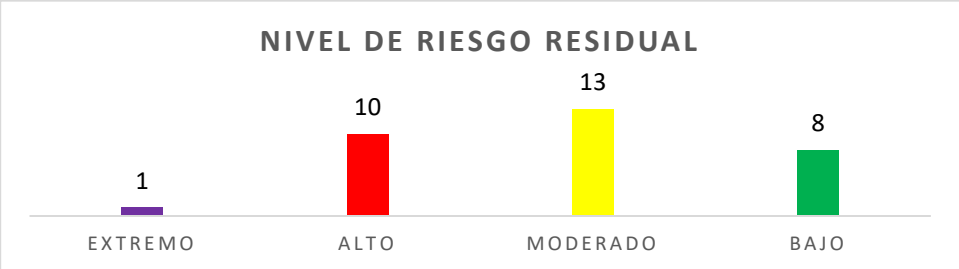

Imagen No. 1-Nivel de Riesgo Residual de los riesgos identificados y actualizados para la vigencia 2026

8.1. Procesos del Nivel Nacional

En articulación con los Enlaces del Sistema Integrado de Gestión – SIG de cada proceso de la Entidad, se realizó la actualización de las matrices de riesgos de Seguridad de la Información para la vigencia 2026, las cuales incluyen los controles y planes de acción aprobados por los líderes de los procesos. A continuación, se listan los controles y planes de acción por cada proceso del nivel nacional.

8.1.1. Reparación integral

En relación con el proceso de Reparación Integral se identificó un (1) riesgo con nivel de severidad residual "Alto":

Redacción del riesgo	Nivel de Severidad Inherente	Nivel de Severidad Residual	Tratamiento	Comentario Tratamiento
Posibilidad de pérdida económica y reputacional por divulgación o alteración no autorizada de los sistemas de información y/o la información sensible registrada en documento físico o digital a la que se tiene autorización de acceso (Activos críticos asociados), debido a vandalismo o hurto, por ausencia o insuficiencia de controles de acceso al archivo digital, acciones involuntarias y/o deliberadas de usuario por ausencia o insuficiencia en la gestión de eventos de monitoreo o por almacenamiento de información sin protección, acceso no controlado a información sensible / confidencial, desconocimiento de los procedimientos y controles de Seguridad de la Información y/o por omisión o inadecuado proceso de identificación y calificación de los activos de información. *Activos críticos asociados al proceso de Reparación Integral.	**Alto**	**Alto**	Reducir - Mitigación	Se define planes de acción adicionales con el fin de evitar la materialización del riesgo.

Tabla No.2 – Riesgo identificado del proceso de Reparación Integral

Es importante mencionar que, el nivel de severidad residual se determinó teniendo en cuenta los siguientes controles existentes:

Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
El Proceso Reparación Integral como administrador de las herramientas tecnológicas del Proceso, a través de los profesionales designados socializa a los colaboradores para que hagan uso responsable en el acceso y manejo de la información del Proceso Reparación Integral, cada vez que se realicen ajustes que afecten los procesos de las herramientas. **Evidencia:** Envió de correo electrónico con tips de recomendaciones sobre el uso de las herramientas utilizadas por el Proceso. **(A.6.3).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo
El Proceso de Reparación Integral suscribe un "Acuerdo de Confidencialidad" con cada uno de los funcionarios y/o contratistas y/o operadores del Proceso, cuando se requiere acceder a los Sistemas de información y/o Servicios TI, en las que se procesa y/o almacena la información de la Entidad, en caso de NO contar con el ""Acuerdo"", no se asignará usuarios y accesos a la información; En el caso de que se venza el ""Acuerdo"" el usuario será deshabilitado. **Evidencia:** Los acuerdos de confidencialidad suscritos por el Proceso, en caso NO presentarse suscripción de ""Acuerdos"" se deberá contar con un correo enviado al líder del Proceso donde se indique que no se realizaron durante el periodo. **(A.6.6).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo
A través de la herramienta del FRV (Fondo para la reparación de las Víctimas) del Proceso de Reparación Integral, se generan mensajes automáticos de notificación cada vez que el usuario realiza actividades de insertar, actualizar, modificar o eliminar, para que el usuario confirme la acción a realizar. **Evidencia:** Pantallazos de los mensajes que genera la herramienta FRV. **(A.8.34).**	Probabilidad	Preventivo	Automatizado	Documentado	Con registro	Continuo

Tabla No.3 – Controles existentes identificados en la gestión de riesgos de Seguridad de la Información del proceso de Reparación Integral

Adicionalmente, el Proceso de Reparación Integral definió el siguiente plan de acción para el tratamiento del riesgo identificado:

Plan de Acción	Fecha Inicio	Fecha Fin	Responsable
El Proceso de Reparación Integral asistirá y participará en las capacitaciones brindadas por la Oficina de Tecnología de Información (OTI), cada vez que se programen con el fin de dar cumplimiento a la implementación de la política del Sistema de gestión de Seguridad y Privacidad de la información para la prevención de riesgos de seguridad digital y apropiación de conocimientos del SGSI. **Evidencia:** Listas de asistencia de participación del proceso. **(A.6.3).**	2/01/2026	31/12/2026	Equipo de Gestión Integral en la Dirección de reparación Integral.

Tabla No.4 – Plan de acción establecido en la gestión de riesgos de Seguridad de la Información del proceso de Reparación Integral

8.1.2. Direccionamiento Estratégico

En relación con el proceso de Direccionamiento Estratégico se identificó un (1) riesgo con nivel de severidad residual "Alto":

Redacción del riesgo	Nivel de Severidad Riesgo Inherente	Nivel de Severidad Riesgo Residual	Tratamiento	Comentario Tratamiento
Posibilidad de pérdida de disponibilidad de los Activos de Información del Proceso de Direccionamiento Estratégico.	**Alto**	**Alto**	Reducir - Mitigación	Dado el nivel de severidad residual del riesgo no se hace necesario implementar un plan de acción.

Tabla No.5 – Riesgo identificado del proceso de Direccionamiento Estratégico

Es importante mencionar que, el nivel de severidad residual se determinó teniendo en cuenta los siguientes controles existentes:

Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
"El profesional designado de la OAP se encarga de revisar e inactivar los usuarios cada vez que se reportan novedades en los aplicativos administrados por la OAP y el profesional de la OTI verificará las solicitudes de acceso al SharePoint para el almacenamiento de la información En caso de que no se reportes novedades o accesos, se verificara la fecha de terminación del contrato para inactivar el usuario correspondiente. **Evidencia:** Correos electrónicos de reporte de novedades y/o correo de solicitud de reportes de la OAP a los Procesos y Direcciones Territoriales. **(A.5.15, A.5.16, A.8.3, A.8.13, A.5.18).**	Probabilidad	Preventivo	Manual	Sin Documentar	Con registro	Continuo

Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
El profesional designado del proceso gestiona la suscripción del ""Acuerdo de Confidencialidad"" con los funcionarios y Contratistas como control de acceso cada vez que se solicita usuarios a las herramientas tecnológicas en las que se procesa y se almacena la información, de lo contrario no se asignaran usuarios, con le fin de dar cumplimento a las Políticas de Seguridad de la Información definidas por la Entidad. Es importante que los funcionarios, contratistas conozcan las implicaciones que se pueden presentar por el uso inadecuado de la información en aras de obtener un beneficio económico por la atención y orientación a las víctimas. El acceso a los sistemas de información involucrados tendrá como límite el perfil o rol documentado en el acuerdo y la fecha de vencimiento del mismo. **Evidencia:** Formatos de aceptación de Acuerdos de Confidencialidad suscritos por la Dirección Territorial y/o reporte de dicho registro y/o correo del responsable de la Dirección Territorial en el que se indique que para el presente periodo no se suscribieron Acuerdos de Confidencialidad. **(A.6.6).**	Probabilidad	Preventivo	Manual	Sin Documentar	Con registro	Continuo

Tabla No.6 – Controles existentes identificados en la gestión de riesgos de Seguridad de la Información del proceso de Direccionamiento Estratégico

Adicionalmente, el Proceso definió el siguiente plan de acción para el tratamiento del riesgo identificado:

Plan de Acción	Fecha Inicio	Fecha Fin	Responsable
El profesional de la OAP articulará en conjunto con la OTI la para promoción de los lineamientos para la inactivación de usuario. **Evidencias:** Correos electrónicos, Piezas Comunicativas. **(A.5.15, A.5.16, A.5.18).**	02/01/2026	31/12/2026	Enlace SIG del Proceso de Direccionamiento Estratégico o designado por el líder del Proceso.
El profesional de la OAP elaborará estrategias de comunicación en articulación con la OAC o las dependencias que apliquen, para la promoción del SIPLAN+ en la Entidad, a fin de generar cultura de apropiación. **Evidencias:** Correos electrónicos, Piezas Comunicativas. **(A.5.15, A.5.16, A.5.18).**	02/01/2026	31/12/2026	Enlace SIG del Proceso de Direccionamiento Estratégico o designado por el líder del Proceso.

Tabla No.7 – Plan de acción establecido en la gestión de riesgos de Seguridad de la Información del proceso de Direccionamiento Estratégico

8.1.3. Gestión de Talento Humano

En relación con el proceso de Gestión de Talento Humano se identificó un (1) riesgo con nivel de severidad residual "Moderado":

Redacción del riesgo	Nivel de Severidad Riesgo Inherente	Nivel de Severidad Riesgo Residual	Tratamiento	Comentario Tratamiento
Posibilidad de pérdida de confidencialidad de los Activos de Información de Expedientes físicos y Sistema Información KACTUS) del Proceso de Gestión de Talento Humano, debido a la falla o ausencia de controles de acceso a la información del Proceso.	**Moderado**	**Moderado**	Reducir - Mitigación	Se define planes de acción adicionales con el fin de evitar la materialización del riesgo.

Tabla No.8 – Riesgo identificado del proceso de Gestión de Talento Humano

Es importante mencionar que, el nivel de severidad residual se determinó teniendo en cuenta los siguientes controles existentes:

Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
El Proceso de Gestión Talento Humano suscribe un ""Acuerdo de Confidencialidad"" con cada uno de los funcionarios y/o contratistas del Proceso, cuando se requiere acceder a los Sistemas de información y/o Servicios TI en las que se procesa y/o almacena la información de la Entidad, en caso de contar con el ""Acuerdo"", no se asignará accesos ni usuarios; para el caso de que se venza el ""Acuerdo"" el usuario será deshabilitado. Este control permite dar cumplimento a las políticas de seguridad de la información definidas por la entidad, por lo que es importante indicarles a los funcionarios y/o contratistas del Proceso las implicaciones que se pueden presentar por el uso inadecuado de la información en aras de obtener un beneficio económico por la atención y orientación a las víctimas. **Evidencia:** Los Acuerdos de Confidencialidad suscritos por el proceso de Gestión de Talento Humano y/o reporte de dicho registro. En caso de que no se suscriban ""Acuerdos de Confidencialidad"" en el periodo, se deberá enviar correo al líder del Proceso de Gestión de Talento Humano indiciándole que no se suscribieron ""Acuerdos"". **(A.6.6).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo

Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
El Proceso de Gestión de Talento Humano a través del Técnico y/o Auxiliar Administrativo valida la solicitud de los documentos de las historias laborales y confirma autorización de trámite por la Coordinadora de Talento Humano. Solicita la historia laboral al Grupo de Gestión Administrativa y Documental en los formatos respectivos para el préstamo del expediente y de control de los archivos de gestión conforme a las tablas de retención documental. En caso de no contar con la información actualizada en la historia laboral se remite correo a la Coordinadora de Talento Humano, con el fin de identificar la solicitud de la historia laboral con los demás lideres de TH. **Evidencia:** Correo electrónico de solicitud y/o formato de préstamos de documento y/o expediente. En caso de no presentarse solicitud de préstamos de documentos y/o expediente en el periodo, se deberá enviar correo al Lider del Proceso de Gestión de Talento Humano indiciándole que no se recibieron solicitudes de "préstamos de documentos y/o expedientes". **(A.6.1, A.6.2, A.6.5, A.5.9, A.5.11, A.7.10, A.5.37).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo

Tabla No.9 – Controles existentes identificados en la gestión de riesgos de Seguridad de la Información del proceso de Gestión de Talento Humano

Adicionalmente, el Proceso definió el siguiente plan de acción para el tratamiento del riesgo identificado:

Plan de Acción	Fecha Inicio	Fecha Fin	Responsable
"El Proceso de Gestión de Talento Humano debe notificar a los administradores del sistema de Información KACTUS las novedades de los usuarios que hace uso del Sistema Tecnológico KACTUS. **Evidencia:** Correo Electrónico de notificación al administrador de KACTUS sobre las novedades de los usuarios que acceden al Sistema, en caso de presentarse novedades en el periodo, se deberá enviar correo al líder del Proceso de Gestión de Talento Humano indiciándole que no se presentaron novedades. **(A.5.15).**	02/01/2026	31/12/2026	Enlace SIG del Proceso de Direccionamiento Estratégico o designado por el líder del Proceso.

Tabla No.10 – Plan de acción establecido en la gestión de riesgos de Seguridad de la Información del proceso de Gestión de Talento Humano

8.1.4. Registro y Valoración

En relación con el proceso de Registro y Valoración se identificó un (1) riesgo con nivel de severidad residual "Moderado":

Redacción del riesgo	Nivel de Severidad Riesgo Inherente	Nivel de Severidad Riesgo Residual	Tratamiento	Comentario Tratamiento
Posibilidad de pérdida reputacional ante las víctimas y la entidad por alteración y difusión no autorizada de información que reposa en herramientas de gestión o activos físicos de información, debido a una administración inadecuada de perfiles de acceso a modificación o consulta o realizar modificaciones sin el conocimiento de los procedimientos establecidos.	**Alto**	**Moderado**	Reducir - Mitigación	Se define planes de acción adicionales con el fin de evitar la materialización del riesgo.

Tabla No.11 – Riesgo identificado del proceso de Reparación Individual

Es importante mencionar que, el nivel de severidad residual se determinó teniendo en cuenta los siguientes controles existentes:

Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
El Agente General del Procedimiento de Gestión de la Declaración y/o a quien se delegue, realiza la actividad de forma diaria de registro y recepción de la documentación en el archivo Excel ""Formato Base Inicial y Formato Recepción"", donde se registra información relacionada con la recepción y la documentación que ingresa para su trámite de cada declaración. En caso de identificar inconvenientes en la documentación se procede a remitir correo con lo identificado a ministerio público. **Evidencia:** Archivo de Excel Formato Base Inicial y Formato Recepción y/o envió de correo de notificación sobre los hallazgos. **(A.6.8, A.6.8, A.18.2.2, A.5.36).**	Probabilidad	Detectivo	Manual	Documentado	Con registro	Continuo
El líder del procedimiento y/o a quien se delegue, reporta de manera mensual por medio de aplicativo las actualizaciones de información RUV, informan sobre los requerimientos o solicitudes atendidas por medio de aplicativo ARANDA, esto con el fin de monitorear constantemente las solicitudes de actualizaciones de información en el RUV que se presentan en el registro. Esto aplica para las solicitudes que se registren por medio de este aplicativo. En caso de encontrar tipologías de solicitudes nuevas, se realizará mesa de trabajo para identificar ruta de envió o generación de nueva tipología. **Evidencia:** Reporte mensual de los Ticket gestionados por ARANDA y/o acta de reunión. **(A.6.8, A.6.8, A.18.2.2, A.5.36).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Aleatorio

Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
El Líder de cada procedimiento y/o a quien se delegue, cada vez que se requiera cargar la data de producción en la carpeta de SharePoint y/o OneDrive designada para el resguardo, para llevar la trazabilidad de los usuarios que cargue, modifican y eliminan, esto con el fin de tener un control relacionado con quien tiene a cargo la información del proceso y los tiempos que la tiene a su cargo. En caso de requerir permisos en SharePoint se realiza la solicitud cada equipo de trabajo a la Oficina de Tecnologías y de Información -OTI. **Evidencia:** Data de producción por cada procedimiento y/o correo de solicitud de accesos a las carpetas de SharePoint. **(A.8.13).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo
"El equipo de apoyo procedimiento gestión de la declaración brinda apoyo técnico a los funcionarios del Ministerio público o consulados en cuanto al uso adecuado de la herramienta de toma en línea, este acompañamiento se realiza por medio telefónico, correo electrónico, de atención inmediata. en caso de no poder contactar por alguno de estos medios, la entidad dispone de material informativo para que se realice la toma de declaración en línea de manera adecuada y se informara de estos a la oficina que solicite asistencia. **Evidencia:** Correos Electrónicos, registro Formato seguimiento soporte en línea. **(A.6.3).**	Impacto	Correctivo	Manual	Documentado	Con registro	Aleatorio

Tabla No.12 – Controles existentes identificados en la gestión de riesgos de Seguridad de la Información del proceso de Registro y Valoración

Adicionalmente, el Proceso definió el siguiente plan de acción para el tratamiento del riesgo identificado:

Plan de Acción	Fecha Inicio	Fecha Fin	Responsable
"El enlace del SIG de registro y valoración articula con la oficina de tecnologías de la información el desarrollo de una sensibilización en temas de seguridad de la información por medio de capacitaciones o material informativo, esto con el fin de que todos los colaboradores conozcan y se sensibilicen frente al manejo de la información con la que cuenta el proceso y los riesgos a los que se encuentra sujeto el mismo **Evidencia:** acta de reunión de los espacios de sesión y/o material divulga, en caso de no realice los espacios de socialización se genera un correo o documento que indique que no se presentó en el periodo. **(A.6.3).**	02/01/2026	31/12/2026	Enlace SIG del Proceso registro y valoración o designado por el líder del Proceso.

Tabla No.13 – Plan de acción establecido en la gestión de riesgos de Seguridad de la Información del proceso de Registro y Valoración

8.1.5. Gestión Documental

En relación con el proceso de Gestión Documental se identificó un (1) riesgo con nivel de severidad residual "Alto":

Redacción del riesgo	Nivel de Severidad Riesgo Inherente	Nivel de Severidad Riesgo Residual	Tratamiento	Comentario Tratamiento
Posibilidad de pérdida de disponibilidad para acceder a la información custodiada por el Proceso de Gestión Documental, debido a la falla o ausencia de controles de seguridad relacionados con los expedientes físicos y electrónicos que se encuentran almacenados en el archivo de gestión, archivo central y el Sistema de Gestión de Documentos Electrónicos de Archivo (ArchiDhu).	**Extremo**	**Alto**	Reducir - Mitigación	Se define planes de acción adicionales con el fin de evitar la materialización del riesgo.

Tabla No.14 – Riesgo identificado del proceso de Gestión Documental

Es importante mencionar que, el nivel de severidad residual se determinó teniendo en cuenta los siguientes controles existentes:

Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
"El Proceso de Gestión Documental, realiza la ""Digitalización de los documentos"" en el Sistema de Gestión de Documentos Electrónicos de Archivo ""ARCHIDU"" para garantizar y facilitar el acceso a la información y con ello evitar la consulta de documentos físicos originales. **Evidencia:** Informe de expedientes digitalizados para el periodo. **(A.5.13, A.5.15, A.8.15).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo
El Proceso de Gestión Documental, genera un inventario documental por dependencia y direcciones territoriales para llevar el registro de los expedientes que se encuentra en el archivo de gestión y archivo central de la Entidad. **Evidencia:** Archivo de Excel del inventario documental por dependencia y Direcciones Territoriales. **(A.5.10, A.5.12, A.5.13, A.5.15, A.8.15).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo

Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
El Proceso de Gestión Documental, cuando se genera una denuncia por pérdidas de un documento o expediente o cuando se identifica que los expedientes no están completos, se aplica el procedimiento para la reconstrucción de expedientes. **Evidencia:** Cuando se reporte una denuncia por pérdida de un expediente y se requiera realizar una reconstrucción de este se debe presentar el informe de pérdida de documento. En los casos en que no se presente reporte por pérdida se deberá enviar un correo al líder del proceso indicando que no se presentó novedades de perdida de expedientes durante el período. **(A.5.33, A.8.15).**	Impacto	Correctivo	Manual	Documentado	Con registro	Aleatorio

Tabla No.15 – Controles existentes identificados en la gestión de riesgos de Seguridad de la Información del proceso de Gestión Documental

Adicionalmente, el Proceso definió el siguiente plan de acción para el tratamiento del riesgo identificado:

Plan de Acción	Fecha Inicio	Fecha Fin	Responsable
El Proceso de Gestión Documental, lleva el registro y control de préstamos de expedientes a los funcionarios y/o contratistas de la Entidad para la atención y trámites en sus dependencias del nivel nacional. **Evidencia:** Formato Préstamo de Documentos y/o Expedientes de Archivos de Gestión mensual. **(A.5.10, A.5.12, A.5.13, A.5.15, A.8.15).**	02/01/2026	31/12/2026	Enlace SIG del Proceso de Gestión Documental o designado por el líder del Proceso.
El Proceso de Gestión Documental, cuenta con las tablas de control para la (Información Pública Reservada, Información Pública Clasificada, Pública) de acuerdo con los lineamientos de Ley 1712 de 2014 para conceder los permisos a los expediente físicos y electrónicos. **Evidencia:** Tablas de control de acceso y/o reporte de configuración de usuarios en ARCHIDhu y/o correos de respuesta de solicitudes de préstamos de expedientes. **(A.5.10, A.5.12, A.5.13).**	02/01/2026	31/12/2026	Enlace SIG del Proceso de Gestión Documental o designado por el líder del Proceso.

Tabla No.16 – Plan de acción establecido en la gestión de riesgos de Seguridad de la Información del proceso de Gestión Documental

8.1.6. Gestión Financiera

En relación con el proceso de Gestión Financiera se identificaron dos (2) riesgos con nivel de severidad residual "Moderado" respectivamente:

Redacción del riesgo	Nivel de Severidad Riesgo Inherente	Nivel de Severidad Riesgo Residual	Tratamiento	Comentario Tratamiento
Posibilidad de pérdida económica y reputacional por manipulación no autorizada de operaciones financieras en el Sistema Integrado de Información Financiera – SIIF Nación, debido a la pérdida o uso indebido del Token asignado a los usuarios autorizados.	**Moderado**	**Moderado**	Reducir - Mitigación	Se define planes de acción adicionales con el fin de evitar la materialización del riesgo.
Posibilidad de pérdida de disponibilidad por la modificación o pérdida de la información física o electrónica de la información del Proceso de Gestión Financiera, debido a la falla o ausencia de controles de seguridad.	**Moderado**	**Moderado**	Reducir - Mitigación	Dado el nivel de severidad residual del riesgo no se hace necesario implementar un plan de acción.

Tabla No.17 – Riesgo identificado del proceso de Gestión Financiera

Es importante mencionar que, el nivel de severidad residual se determinó teniendo en cuenta los siguientes controles existentes:

Redacción del riesgo	Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
Posibilidad de pérdida económica y reputacional por manipulación no autorizada de operaciones financieras en el Sistema Integrado de Información Financiera – SIIF Nación, debido a la pérdida o uso indebido del Token asignado a los usuarios autorizados.	El Proceso de Gestión Financiera suscribe un ""Acuerdo de Confidencialidad"" con cada uno de los funcionarios y/o contratistas del Proceso, cuando se requiere acceder a los Sistemas de información y/o Servicios TI en las que se procesa y/o almacena la información de la Entidad, en caso de contar con el ""Acuerdo"", no se asignará accesos ni usuarios; para el caso de que se venza el ""Acuerdo"" el usuario será deshabilitado. Este control permite dar cumplimento a las políticas de seguridad de la información definidas por la entidad, por lo que es importante indicarles a los funcionarios y/o contratistas del Proceso las implicaciones que se pueden presentar por el uso inadecuado de la información en aras de obtener un beneficio económico por la atención y orientación a las víctimas. **Evidencia:** Los Acuerdos de Confidencialidad suscritos por el proceso de Gestión de Financiera y/o reporte de dicho registro. En caso de no presentar suscripción de ""Acuerdos de Confidencialidad"", se deberá enviar correo al líder del proceso indicándoles que no se suscribieron acuerdos **(A.6.6).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo

Redacción del riesgo	Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
	El Proceso de Gestión Financiera aplica el formato de responsabilidad de uso de la firma digital por medio del TOKEN el cual es asignado a funcionarios y/o contratistas específicos para la ejecución de las actividades propias del Proceso. **Evidencia:** Diligenciamiento del formato de responsabilidad. En caso de que no asigne un TOKEN a un colaborador, se deberá enviar correo al líder del proceso indicándoles que no se presentó asignación de TOKEN. **(A.6.6).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo
Posibilidad de pérdida de disponibilidad por la modificación o pérdida de la información física o electrónica de la información del Proceso de Gestión Financiera, debido a la falla o ausencia de controles de seguridad.	El Proceso de Gestión Financiera realiza el control para el préstamo de documentos físicos o digitales del proceso a través de una solicitud por correo electrónico. Para el préstamo de archivos físicos se realiza el envío del correo a Gestión Documental y para el préstamo de archivos digitales (internos) del proceso se realiza la solicitud al profesional o apoyo de archivo de Gestión financiera. **Evidencia:** Envió de la solicitud a través de correo electrónico. En caso de que no se reciban solicitudes de préstamos de archivos durante el período, se deberá enviar correo al líder del proceso indicándoles que no se recibieron solicitudes de préstamo de documentos en el período correspondiente al seguimiento. **(A.5.2, A.5.3, A.5.4, A.5.10, A.5.11, A.5.15, A.5.33).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo
	"El Proceso de Gestión Financiera establece el uso de las herramientas SharePoint y/o OneDrive para el almacenamiento de la información electrónica que administra. Para efectos de verificación, se tomará una muestra equivalente al 10% de los colaboradores, con el fin de evidenciar la utilización de dichas herramientas. **Evidencia:** Capturas de pantalla y/o registros fotográficos que evidencien el uso de SharePoint y/o OneDrive en los equipos de cómputo del proceso durante el periodo reportado **(A.5.16, A.8.2, A.8.3, A.8.13).**	Probabilidad	Preventivo	Manual	Sin Documentar	Con registro	Continuo

Tabla No.18 – Controles existentes identificados en la gestión de riesgos de Seguridad de la Información del proceso de Gestión Financiera

Adicionalmente, el Proceso definió el siguiente plan de acción para el tratamiento del riesgo identificado:

Plan de Acción	Fecha Inicio	Fecha Fin	Responsable
"El Proceso de Gestión Financiera notifica al administrador del SIIF de la Entidad las novedades del funcionario y/o contratista para que se inactive el usuario. En caso de no presentarse novedad el Proceso de Gestión Financiera deberá reportar un correo indicando que no se presentaron novedades. **Evidencia:** correo de notificación de la novedad para inactivación del acceso al usuario o correo de notificación indicando que no se presentó novedades. **(A.6.2, A.6.3, A.6.5, A.6.6).**	02/01/2026	31/12/2026	Enlace SIG del Grupo de Gestión Financiera o designado por el líder del Proceso.
El Proceso de Gestión Financiera enviara una notificación para que los procesos que interactúan con SIIF reporte novedades de usuarios SIIF (desvinculación, vacaciones, incapacidades, entre otros). **Evidencia:** Correo o memorando o circular a los procesos que interactúan con SIIF. **(A.6.2, A.6.3, A.6.5, A.6.6).**	02/01/2026	31/12/2026	Enlace SIG del Grupo de Gestión Financiera o designado por el líder del Proceso.
"El Proceso de Gestión Financiera deberá asistir y participar en las capacitaciones programadas por la Oficina de Tecnología de la Información (OTI), con el fin de dar cumplimiento a la política del Sistema de Gestión de Seguridad de la Información, fortalecer los controles de seguridad, prevenir la pérdida o modificación de la información y garantizar la disponibilidad de los datos del Proceso de Gestión Financiera. **Evidencia:** Correo electrónico de invitación a las charlas de seguridad de la información, replicadas por el enlace del proceso, y listado de asistencia correspondiente. **(A.6.2, A.6.3, A.6.5, A.6.6).**	02/01/2026	31/12/2026	Enlace SIG del Grupo de Gestión Financiera o designado por el líder del Proceso.

Tabla No.19 – Plan de acción establecido en la gestión de riesgos de Seguridad de la Información del proceso de Gestión Financiera

8.1.7. Gestión Administrativa

En relación con el proceso de Gestión Administrativa se identificaron dos (2) riesgos con nivel de severidad residual "Bajo":

Redacción del riesgo	Nivel de Severidad Riesgo Inherente	Nivel de Severidad Riesgo Residual	Tratamiento	Comentario Tratamiento
Posibilidad de pérdida económica y reputacional por pérdida de la Confidencialidad de la Información de la Entidad, debido a la falta de controles de acceso físico y perimetrales de las instalaciones de la Entidad, por ingreso de personal no autorizado.	**Moderado**	**Bajo**	Aceptar	Dado el nivel de severidad residual del riesgo no se hace necesario implementar un plan de acción, pero el proceso define un plan de acción adicionales con el fin de evitar la materialización del riesgo.
Posibilidad de pérdida de disponibilidad y/o continuidad del Servicio eléctrico, debido a falta o ausencia de mantenimiento preventivo de la planta eléctrica y ups del complejo empresarial San Cayetano donde opera la Entidad.	**Moderado**	**Bajo**	Aceptar	Dado el nivel de severidad residual del riesgo no se hace necesario implementar un plan de acción.

Tabla No.20 – Riesgo identificado del proceso de Gestión Administrativa

Es importante mencionar que, el nivel de severidad residual se determinó teniendo en cuenta los siguientes controles existentes:

Redacción del riesgo	Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
Posibilidad de pérdida económica y reputacional por pérdida de la Confidencialidad de la Información de la Entidad, debido a la falta de controles de acceso físico y perimetrales de las instalaciones de la Entidad, por ingreso de personal no autorizado.	El Proceso de Gestión Administrativa realiza la contratación de Vigilancia, con el fin preservar la seguridad de los activos de información y los Colaboradores de la Entidad. Evidencia: Contrato de Vigilancia. **(A.5.21, A.5.23, A.5.36, A.7.4, A.7.11).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo
	"El Proceso de Gestión Administrativa, define como mecanismo de control para el acceso de personal a las instalaciones de la Entidad, el registro en la herramienta ""Ingreso San Cayetano Power App"" por parte de las áreas que requieran la autorización de ingreso. **Evidencia:** Registro de la herramienta y/o informe y/o correo de generación de la solicitud de las áreas que requieran autorización de ingreso. **(A.5.21, A.5.23, A.5.36, A.7.4, A.7.11).**	Probabilidad	Preventivo	Automatizado	Documentado	Con registro	Continuo

Redacción del riesgo	Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
	El Proceso de Gestión Administrativa, define plan de choque cuando se materialice el riesgo de la vulneración de la seguridad mediante el consumo de utilización de servicios adicionales de seguridad que son templados en la proyección del desarrollo del contrato vigente. **Evidencia:** Correos de solicitud de servicios adicionales (personal de apoyo) y/o trazabilidad en el software de vigilancia y del monitoreo de vigilancia por parte de la Entidad del complejo sobre el ingreso del personal que apoyo a la eventualidad. **(A.5.21, A.5.23, A.5.36, A.7.4, A.7.11).**	Impacto	Correctivo	Manual	Documentado	Con registro	Aleatorio
Posibilidad de pérdida de disponibilidad y/o continuidad del Servicio eléctrico, debido a falta o ausencia de mantenimiento preventivo de la planta eléctrica y ups del complejo empresarial San Cayetano donde opera la Entidad.	El Proceso de Gestión Administrativa, realiza el seguimiento a la Administración del Complejo San Cayetano donde opera la Entidad, frente al cumplimiento de las pruebas y mantenimiento de la planta eléctrica de manera bimestral con el objetivo de garantizar la Continuidad del Servicio y tomar medidas correctivas. **Evidencia:** Envío del correo electrónico bimestral del Proceso de Gestión Administrativa a la Administración del Complejo para el seguimiento del cronograma de las pruebas y mantenimiento de la planta eléctrica ejecutadas por la Administración del Complejo. **(A.5.21, A.5.23, A.5.36, A.7.4, A.7.11).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo
	El Proceso de Gestión Administrativa, realiza el seguimiento a la Administración del Complejo San Cayetano donde opera la Entidad, frente al cumplimiento de las pruebas y mantenimiento de la UPS de manera bimestral con el objetivo de garantizar la Continuidad del Servicio y tomar medidas correctivas. **Evidencia:** Envío del correo electrónico bimestral del Proceso de Gestión Administrativa a la Administración del Complejo para el seguimiento del cronograma de las pruebas y mantenimiento de la UPS ejecutadas por la Administración del Complejo. **(A.5.21, A.5.23, A.5.36, A.7.4, A.7.11).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo

Redacción del riesgo	Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
	El Proceso de Gestión Administrativa, en caso de identificar que no se están realizando las actividades de las pruebas y mantenimientos preventivos para la planta eléctrica y UPS donde opera la Entidad, se procederá a realizar un comunicado a la Administración del Complejo San Cayetano frente a las fallas presentadas en la continuidad del servicio eléctrico. **Evidencia:** Envió de correo electrónico del Proceso de Gestión Administrativa por el incumplimiento de las pruebas y mantenimientos de la planta eléctrica y UPS a la Administración del Complejo San Cayetano donde opera la entidad. **(A.5.21, A.5.23, A.5.36, A.7.4, A.7.11).**	Impacto	Correctivo	Manual	Documentado	Con registro	Continuo

Tabla No.21 – Controles existentes identificados en la gestión de riesgos de Seguridad de la Información del proceso de Gestión Administrativa

Adicionalmente, el Proceso definió el siguiente plan de acción para el tratamiento del riesgo identificado:

Plan de Acción	Fecha Inicio	Fecha Fin	Responsable
"El Proceso de Gestión Administrativa, realiza el seguimiento mensual al Proveedor de Vigilancia con fin de verificar el cumplimiento de las actividades enmarcadas en el Contrato. **Evidencia:** Informe de ejecución del contrato de vigilancia. **(A.5.21, A.5.23, A.5.36, A.7.4, A.7.11).**	01/01/2026	31/12/2026	Enlace SIG del Proceso Gestión Administrativa o designado por el líder del Proceso.

Tabla No.22 – Plan de acción establecido en la gestión de riesgos de Seguridad de la Información del proceso de Gestión Administrativa

8.1.8. Gestión Contractual

En relación con el proceso de Gestión Contractual se identificaron dos (2) riesgos con nivel de severidad residual "Alto" y "Moderado" respectivamente:

Redacción del riesgo	Nivel de Severidad Riesgo Inherente	Nivel de Severidad Riesgo Residual	Tratamiento	Comentario Tratamiento
Posibilidad de pérdida económica y reputacional por pérdida a la Confidencialidad de la Información de la Entidad debido a la falla o ausencia de controles relacionados con el acceso a información clasificada y/o reservada.	**Alto**	**Alto**	Reducir - Mitigación	Se define planes de acción adicionales con el fin de evitar la materialización del riesgo.
Posibilidad de pérdida económica y reputacional por pérdida de la Disponibilidad de la Información de la Entidad debido a la falla o ausencia de controles de seguridad aplicables.	**Moderado**	**Moderado**	Reducir - Mitigación	Se define planes de acción adicionales con el fin de evitar la materialización del riesgo.

Tabla No.23 – Riesgo identificado del proceso de Gestión Contractual

Es importante mencionar que, el nivel de severidad residual se determinó teniendo en cuenta los siguientes controles existentes:

Redacción del riesgo	Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
Posibilidad de pérdida económica y reputacional por pérdida a la Confidencialidad de la Información de la Entidad debido a la falla o ausencia de controles relacionados con el acceso a información clasificada y/o reservada.	"El Proceso de Gestión Contractual suscribe un ""Acuerdo de Confidencialidad"" con cada uno de los funcionarios y/o contratistas del Proceso cuando se requiere acceder a los sistemas de información y/o servicios TI en los que se procesa y/o almacena la información de la entidad. En caso de no contar con el ""Acuerdo"", no se asignarán accesos ni usuarios. Para el caso de que se venza el ""Acuerdo"", el usuario será deshabilitado. Este control permite dar cumplimiento a las políticas de seguridad de la información definidas por la entidad, por lo que es importante indicarles a los funcionarios y/o contratistas del Proceso las implicaciones que se pueden presentar por el uso inadecuado de la información con el fin de obtener un beneficio económico a través de la atención y orientación a las víctimas. **Evidencia:** Los Acuerdos de Confidencialidad suscritos por el proceso de Gestión Contractual y/o reporte de dicho registro. **(A.6.6).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo

Redacción del riesgo	Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
	El Proceso de Gestión Contractual firma un Acuerdo de Confidencialidad con Gestión Documental para el cargue y descarga de expedientes contractuales de la herramienta ARCHIDU. **Evidencia:** Los Acuerdos de Confidencialidad de ARCHIDU suscritos por el proceso de Gestión Contractual. **(A.6.6).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo
Posibilidad de pérdida económica y reputacional por pérdida de la Disponibilidad de la Información de la Entidad debido a la falla o ausencia de controles de seguridad aplicables.	El Proceso de Gestión Contractual realiza la entrega formal de los expedientes físicos y digitales al Proceso de Gestión Documental a través de memorandos (radicados), correos electrónicos con aval del GGAD y FUID. **Evidencia:** Los memorandos (radicados), correos electrónicos con aval del GGAD y FUID. **(A.5.9, A.5.10, A.5.11).**	Probabilidad	Preventivo	Automatizado	Documentado	Con registro	Continuo
	El Proceso de Gestión Contractual realiza la publicación de la etapa precontractual y post contractual en el aplicativo SECOP, con el fin de tener la información disponible y actualizada de los procesos ejecutados. **Evidencia:** Se relacionarán los números de procesos ejecutados en el aplicativo SECOP. **(A.8.8).**	Probabilidad	Preventivo	Automatizado	Documentado	Con registro	Continuo

Tabla No.24 – Controles existentes identificados en la gestión de riesgos de Seguridad de la Información del proceso de Gestión Contractual

Adicionalmente, el Proceso definió el siguiente plan de acción para el tratamiento del riesgo identificado:

Plan de Acción	Fecha Inicio	Fecha Fin	Responsable
El enlace SIG del Proceso de Gestión Contractual deberá socializar los compromisos y el estado actual del Sistema de Gestión de Seguridad de la Información (SGSI) en cada uno de los encuentros ""Enlace SIG"", y retroalimentar la información generada por parte de la Oficina de Tecnología de la Información (OTI) en materia de seguridad, la cual es publicada en la intranet. Además, deberá promover la participación, al interior del Proceso, en las charlas de seguridad convocadas. **Evidencia:** Correos electrónicos con socializaciones, inducciones, guías, instructivos e invitaciones enviadas por el Sistema de Gestión de Seguridad de la Información (SGSI) y socializadas al interior del GGC. **(A.6.3).**	02/01/2026	31/12/2026	Enlace SIG del Grupo de Gestión Contractual o designado por el líder del Proceso.

Plan de Acción	Fecha Inicio	Fecha Fin	Responsable
El Proceso de Gestión Contractual retroalimenta a los funcionarios y contratistas respecto al reporte emitido por la Oficina de Tecnología de la Información (OTI) sobre el estado de uso de OneDrive. **Evidencia:** Socialización del correo electrónico enviado por la OTI sobre el estado del uso de OneDrive del Proceso. **(A.5.16, A.8.2, A.8.3, A.8.13).**	02/01/2026	31/12/2026	Enlace SIG del Grupo de Gestión Contractual o designado por el líder del Proceso.

Tabla No.25 – Plan de acción establecido en la gestión de riesgos de Seguridad de la Información del proceso de Gestión Contractual

8.1.9. Gestión Jurídica

En relación con el proceso de Gestión Jurídica se identificaron dos (2) riesgos con nivel de severidad residual "Moderado" y "Alto" respectivamente:

Redacción del riesgo	Nivel de Severidad Riesgo Inherente	Nivel de Severidad Riesgo Residual	Tratamiento	Comentario Tratamiento
Posibilidad de pérdida económica y reputacional por pérdida de la Confidencialidad de la Información de la Entidad debido a la falla o ausencia de controles relacionados con el acceso a información clasificada y/o reservada.	**Alto**	**Moderado**	Reducir - Mitigación	Se define planes de acción adicionales con el fin de evitar la materialización del riesgo.
Posibilidad de pérdida económica y reputacional por pérdida de la Disponibilidad de la Información de la Entidad debido a la falla o ausencia de controles de seguridad aplicables.	**Alto**	**Alto**	Reducir - Mitigación	Se define planes de acción adicionales con el fin de evitar la materialización del riesgo.

Tabla No.26 – Riesgo identificado del proceso de Gestión Jurídica

Es importante mencionar que, el nivel de severidad residual se determinó teniendo en cuenta los siguientes controles existentes:

Redacción del riesgo	Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
Posibilidad de pérdida económica y reputacional por pérdida de la Confidencialidad de la Información de la Entidad debido a la falla o ausencia de controles relacionados con el acceso a información clasificada y/o reservada.	El Proceso de Gestión Jurídica suscribe un ""Acuerdo de Confidencialidad"" con cada uno de los funcionarios y/o contratistas del Proceso, cuando se requiere acceder a los Sistemas de información y/o Servicios TI en las que se procesa y/o almacena la información de la Entidad, en caso de contar con el ""Acuerdo"", no se asignará accesos ni usuarios; para el caso de que se venza el ""Acuerdo"" el usuario será deshabilitado. Este control permite dar cumplimento a las políticas de seguridad de la información definidas por la entidad, por lo que es importante indicarles a los funcionarios y/o contratistas del Proceso las implicaciones que se pueden presentar por el uso inadecuado de la información en aras de obtener un beneficio económico por la atención y orientación a las víctimas. **Evidencia:** Los Acuerdos de Confidencialidad suscritos por el proceso de Gestión de Jurídica y/o reporte de dicho registro. **(A.6.6).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo
	El Proceso de Gestión Jurídica notifica al administrador de los Sistemas de Información (LEX) de la Entidad y a la Oficina de Tecnología de la Información (OTI) las novedades del funcionario y/o contratista para que se inactive el usuario. En caso de no presentarse novedad el Proceso de Gestión Jurídica deberá reportar un correo indicando que no se presentó novedades en el periodo. **Evidencia:** correo de notificación de la novedad para inactivación del acceso al usuario o correo de notificación indicando que no se presentó novedades en el período. **(A.6.2, A.6.3, A.6.5, A.6.6).**	Impacto	Correctivo	Manual	Sin Documentar	Con registro	Continuo
Posibilidad de pérdida económica y reputacional por pérdida de la Disponibilidad de la Información de la Entidad debido a la falla o ausencia de controles de seguridad aplicables.	El Proceso de Gestión Jurídica documenta mediante muestra del 10% del recurso humano, la configuración y uso de OneDrive en lo equipos de cómputo asignados por la Oficina de TI. **Evidencia:** Capturas de pantalla y/o fotografías donde se evidencie la configuración y uso de OneDrive en equipos de cómputo durante el periodo reportado. **(A.5.16, A.8.2, A.8.3, A.8.13).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo

Redacción del riesgo	Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
	El Proceso de Gestión Jurídica en articulación con la Oficina de TI gestiona las novedades de acceso a los usuarios para (consulta, adición y modificación) de la información en la herramienta de SharePoint del Proceso. En caso de no presentarse novedades en el periodo de seguimiento, debe documentarse la situación mediante correo dirigido al Líder del Proceso. **Evidencia:** Correo de solicitud a la OTI para conocer los permisos asociados al SharePoint del Proceso. **(A.5.2, A.5.3, A.5.15).**	Probabilidad	Preventivo	Manual	Sin Documentar	Con registro	Continuo

Tabla No.27 – Controles existentes identificados en la gestión de riesgos de Seguridad de la Información del proceso de Gestión Jurídica

Adicionalmente, el Proceso definió el siguiente plan de acción para el tratamiento del riesgo identificado:

Plan de Acción	Fecha Inicio	Fecha Fin	Responsable
El Proceso de Gestión de Jurídica deberá asistir y participar en las capacitaciones brindadas por la Oficina de Tecnología de Información (OTI), cada vez que se programen con el fin de dar cumplimiento a la implementación de la política del Sistema de gestión de seguridad y privacidad de información, prevención de riesgos de seguridad digital y apropiación de conocimientos del SGSI. **Evidencia:** Correo electrónico con invitación a participar en las charlas de seguridad de la información replicados por el enlace del proceso y lista de asistencia. **(A.6.3).**	01/01/2026	31/12/2026	Enlace SIG del Grupo de Gestión Jurídica o designado por el líder del Proceso.
El Proceso de Gestión Jurídica en articulación con la Oficina de Tecnología de la Información (OTI) gestionará jornadas de concientización o socialización para el uso de herramientas tecnológicas disponibles en la Entidad para el aseguramiento de la Información del Proceso. **Evidencia:** Actas de reunión y listas de asistencia. **(A.8.26, A.8.29, A.8.31).**	01/01/2026	31/12/2026	Enlace SIG del Grupo de Gestión Jurídica o designado por el líder del Proceso.

Tabla No.28 – Plan de acción establecido en la gestión de riesgos de Seguridad de la Información del proceso de Gestión Jurídica

8.1.10. Control Interno Disciplinario

En relación con el proceso de Control Interno Disciplinario se identificaron dos (2) riesgos con nivel de severidad residual "Moderado" y "Alto" respectivamente:

Redacción del riesgo	Nivel de Severidad Riesgo Inherente	Nivel de Severidad Riesgo Residual	Tratamiento	Comentario Tratamiento
Posibilidad de pérdida económica y reputacional por pérdida de la Confidencialidad de la Información de la Entidad, debido a la falla o ausencia de controles relacionados con el acceso a información clasificada y/o reservada.	**Moderado**	**Moderado**	Reducir - Mitigación	Se define planes de acción adicionales con el fin de evitar la materialización del riesgo.
Posibilidad de pérdida económica y reputacional por pérdida de la Disponibilidad de la Información de la Entidad, debido a la falla o ausencia de controles de seguridad aplicables.	**Bajo**	**Bajo**	Aceptar	Dado el nivel de severidad residual del riesgo no se hace necesario implementar un plan de acción

Tabla No.29 – Riesgo identificado del proceso de Control Interno Disciplinario

Es importante mencionar que, el nivel de severidad residual se determinó teniendo en cuenta los siguientes controles existentes:

Redacción del riesgo	Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
Posibilidad de pérdida económica y reputacional por pérdida de la Confidencialidad de la Información de la Entidad, debido a la falla o ausencia de controles relacionados con el acceso a información clasificada y/o reservada.	El Proceso de Control Interno Disciplinario suscribe un ""Acuerdo de Confidencialidad"" de usuarios de aplicativos, herramientas o información, con cada uno de los funcionarios y/o contratistas del Proceso, para acceder a la información del proceso y de la Entidad, en caso de no contar con el ""Acuerdo"", no se asignarán accesos ni usuarios; en los casos en los que se termine la contratación o por renuncia de algún colaborador los usuarios serán deshabilitados. **Evidencia:** Los Acuerdos de Confidencialidad suscritos por el proceso de Control Interno Disciplinario y/o reporte de dicho registro. **(A.6.6).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo

Redacción del riesgo	Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
	Los funcionarios y/o contratistas de Proceso de Control Interno Disciplinario, son responsables de salvaguardar la información de los expedientes físicos a su cargo. Cuando alguno de los funcionarios y colaboradores requieran el ingreso al archivo físico, se realizará la solicitud a la persona delegada por el proceso mediante el registro de la planilla de ingreso y/o envío de correo electrónico. En caso de que el usuario no reporte el ingreso al archivo físico, la persona designada enviará correo en el que se recuerde que se debe dar cumplimiento de los lineamientos establecidos al interior del proceso. **Evidencia:** Registro de la planilla de ingreso y/o envío de correo electrónico y/o correos recordatorios de cumplimiento de lineamientos. **(A.7.2).**	Probabilidad	Detectivo	Manual	Sin Documentar	Con registro	Continuo
Posibilidad de pérdida económica y reputacional por pérdida de la Disponibilidad de la Información de la Entidad, debido a la falla o ausencia de controles de seguridad aplicables.	El Proceso de Control Interno Disciplinario retroalimenta a los funcionarios y contratistas frente al reporte emitido por la Oficina de Tecnología de Información (OTI) sobre el estado de uso de OneDrive. **Evidencia:** Socialización del correo electrónico enviado por la OTI sobre el estado del uso de OneDrive de Proceso. **(A.5.16, A.8.2, A.8.3, A.8.13).**	Probabilidad	Preventivo	Automatizado	Documentado	Con registro	Continuo

Tabla No.30 – Controles existentes identificados en la gestión de riesgos de Seguridad de la Información del proceso de Control Interno Disciplinario

Adicionalmente, el Proceso definió el siguiente plan de acción para el tratamiento del riesgo identificado:

Plan de Acción	Fecha Inicio	Fecha Fin	Responsable
Por parte del Coordinador del Grupo de Control Interno Disciplinario se solicitará una reunión para que, desde la Oficina de Tecnologías de la Información, se garantice la salvaguarda de la información del proceso, que se encuentra guardada en One Drive, dentro de la cual se busca contar con niveles de acceso de acuerdo con los roles de los funcionarios del grupo asignados para esto. Adicionalmente, se solicitará a la OTI mapeo de los nombres de las personas que hayan ingresado a One Drive y que correspondan solamente a funcionarios y colaboradores autorizados del grupo Control Interno Disciplinario. **Evidencia:** quedará Acta de Reunión y compromisos. **(A.5.16, A.8.2, A.8.3, A.8.13).**	02/01/2026	31/12/2026	Enlace SIG de Control Interno Disciplinario o designado por el líder del Proceso.

Tabla No.31 – Plan de acción establecido en la gestión de riesgos de Seguridad de la Información del proceso de Control Interno Disciplinario

8.1.11. Evaluación Independiente

En relación con el proceso de Evaluación Independiente se identificaron dos (2) riesgos con nivel de severidad residual "Bajo":

Redacción del riesgo	Nivel de Severidad Riesgo Inherente	Nivel de Severidad Riesgo Residual	Tratamiento	Comentario Tratamiento
Posibilidad de pérdida reputacional por Incumplimiento de la aplicación de las políticas de seguridad de la Información, por el desconocimiento de las herramientas y controles tecnológicos disponibles para la adecuada gestión de la información que gestiona la Oficina de Control Interno. lo anterior se presenta por la falta de cultura organizacional en torno a la seguridad de la información, reflejada en la falta de capacitación, sensibilización y apropiación de las políticas de seguridad de la información y herramientas tecnológicas dispuestas por la Entidad.	**Moderado**	**Bajo**	Aceptar	En consideración al nivel de severidad residual del riesgo, no se requiere la implementación de un plan de acción adicional.
Posibilidad de pérdida reputacional por la divulgación no autorizada de información que gestiona la Oficina de Control Interno, debido al no cumplimiento de las normas de auditorías generalmente aceptadas de la prudencia y reserva de la información y la generación de conflictos de intereses por parte de los auditores de la OCI, lo anterior por la falta de ética de los auditores.	**Moderado**	**Bajo**	Aceptar	En consideración al nivel de severidad residual del riesgo, no se requiere la implementación de un plan de acción adicional.

Tabla No.32 – Riesgo identificado del proceso de Evaluación Independiente

Es importante mencionar que, el nivel de severidad residual se determinó teniendo en cuenta los siguientes controles existentes:

Redacción del riesgo	Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
Posibilidad de pérdida reputacional por Incumplimiento de la aplicación de las políticas de seguridad de la Información, por el desconocimiento de las herramientas y controles tecnológicos disponibles para la adecuada gestión de la información que gestiona la Oficina de Control Interno. lo anterior se presenta por la falta de cultura organizacional en torno a la seguridad de la información, reflejada en la falta de capacitación, sensibilización y apropiación de las políticas de seguridad de la información y herramientas tecnológicas dispuestas por la Entidad.	El profesional en Ingeniería de Sistemas de la Oficina de Control Interno será responsable de planificar y ejecutar capacitaciones y jornadas de sensibilización sobre las políticas del Sistema de Gestión de Seguridad de la Información (SGSI) y el uso adecuado de las herramientas tecnológicas institucionales. Estas actividades se desarrollarán de manera trimestral con el propósito de fortalecer el conocimiento y la apropiación de los lineamientos de seguridad de la información establecidos por la OCI. En caso de no realizarse en la fecha prevista, la capacitación deberá ser reprogramada oportunamente. **Evidencia de su cumplimiento:** listas de asistencia correo de citación de la sesión y memoria técnica. **(Referencia: A.6.3).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo
Posibilidad de pérdida reputacional por la divulgación no autorizada de información que gestiona la Oficina de Control Interno, debido al no cumplimiento de las normas de auditorías generalmente aceptadas de la prudencia y reserva de la información y la generación de conflictos de intereses por parte de los auditores de la OCI, lo anterior por la falta de ética de los auditores.	El profesional en Ingeniería de Sistemas de la Oficina de Control Interno será responsable realizar los acuerdos de Confidencialidad de todos los funcionarios y contratistas adscritos a la Oficina de Control Interno de manera anual y conforme a las necesidades que se presenten en la vigencia con el objetivo de brindar acceso a los sistemas de información o a herramientas colaborativas de la Entidad (como OneDrive y SharePoint), en las cuales se procesa y/o almacena información institucional, en caso de no suscribir este documento se informara al líder del proceso para tomar las acciones correctivas. Evidencia: Acuerdos de Confidencialidad firmados y archivados. Referencia: (A.6.6)	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo
	"La Oficina de Control Interno a través de sus funcionarios o contratistas realizara capacitaciones o sensibilizaciones de manera trimestral sobre la confidencialidad, disponibilidad e integridad de la información y demás temas relacionados con gestión de la información con el propósito de fortalecer la cultura de la apropiación de las buenas prácticas al interior del proceso, en caso de que no se ejecuten las sesiones se programaran nuevamente para dar cumplimiento al mencionado control. Evidencia: Listas de Asistencia, citación sesión, memoria técnica.	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo

Tabla No.33 – Controles existentes identificados en la gestión de riesgos de Seguridad de la Información del proceso de Evaluación Independiente

El Proceso no definió plan de acción para el tratamiento de los riesgos, toda vez que el nivel de riesgo residual es "Bajo"

8.1.12. Relación con el Ciudadano

En relación con el proceso de Relación con el Ciudadano se identificó un (1) riesgo con nivel de severidad residual "Alto":

Redacción del riesgo	Nivel de Severidad Riesgo Inherente	Nivel de Severidad Riesgo Residual	Tratamiento	Comentario Tratamiento
Posibilidad de pérdida económica y reputacional por pérdida de la Confidencialidad de la Información de la Entidad, Personas inescrupulosas quieren obtener lucro económico por la información de víctimas que reposa en los diferentes aplicativos de la Entidad.	**Alto**	**Alto**	Reducir - Mitigación	Se define planes de acción adicionales con el fin de evitar la materialización del riesgo.

Tabla No.34 – Riesgo identificado del proceso de Relación con el Ciudadano

Es importante mencionar que, el nivel de severidad residual se determinó teniendo en cuenta los siguientes controles existentes:

Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
El Proceso de Relación con el Ciudadano suscribe un ""Acuerdo de Confidencialidad"" con cada uno de los funcionarios y/o contratistas y/o operadores del Proceso, cuando se requiere acceder a los Sistemas de información y/o Servicios TI en las que se procesa y/o almacena la información de la Entidad, en caso de contar con el ""Acuerdo"", no se asignará accesos ni usuarios; para el caso de que se venza el ""Acuerdo"" el usuario será deshabilitado. Este control permite dar cumplimento a las políticas de seguridad de la información definidas por la entidad, por lo que es importante indicarles a los funcionarios y/o contratistas y/o operadores del Proceso las implicaciones que se pueden presentar por el uso inadecuado de la información en aras de obtener un beneficio económico por la atención y orientación a las víctimas. **Evidencia:** Los Acuerdos de Confidencialidad suscritos por el proceso de Relación con el Ciudadano y/o reporte de dicho registro. **(A.6.6).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo

Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
El Proceso de Relación con el Ciudadano de acuerdo con las solicitudes generadas por sospecha de fuga de información, se procede a realizar una actividad de auditoria para validar que usuarios del Sistema de Gestión de víctimas (SGV) están ingresando en horario no permitido, esta actividad se realiza por demanda. **Evidencia:** Correo de sospecha de fuga de información y/o correo de solicitud de eventos afectados en el periodo. **(A.5.15, A.5.33, A.6.8).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Aleatorio
El Proceso de Relación con el Ciudadano envía correo a la Subdirección de Asistencia y Atención Humanitaria solicitando reporte de usuarios inactivos del periodo a reportar (gestionado) de los Sistemas de Información relacionados al Proceso. **Evidencia:** Correo de solicitud del reporte de inactivación y respuesta de la Subdirección de Asistencia Humanitaria. **(A.5.15, A.5.16, A.5.17, A.5.18, 8.3, 8.26).**	Probabilidad	Preventivo	Automatizado	Documentado	Con registro	Continuo

Tabla No.35 – Controles existentes identificados en la gestión de riesgos de Seguridad de la Información del proceso de Relación con el Ciudadano

Adicionalmente, el Proceso definió el siguiente plan de acción para el tratamiento del riesgo identificado:

Plan de Acción	Fecha Inicio	Fecha Fin	Responsable
El Proceso de Relación con el Ciudadano reportará cualquier evento y/o incidente de Seguridad que se presente en el proceso y que afecte la confidencialidad de la información de las víctimas. **Evidencia:** Correos de notificación del evento y/o incidente de seguridad, en caso de que no se presente se genera un correo al líder del proceso indicando que en la vigencia no se presentó eventos y/o incidentes de seguridad de la información. **(A.6.8).**	02/01/2026	31/12/2026	Enlace SIG del Proceso de Relación con el Ciudadano o designado por el líder del Proceso.
Las personas de Servicio al Ciudadano encargadas de los canales de atención generan notas informativas de sensibilización de los temas de seguridad y privacidad de la información a los usuarios de los diferentes canales de atención. **Evidencia:** notas informativas de sensibilización de los temas de seguridad. **(A.6.3).**	02/01/2026	31/12/2026	Enlace SIG del Proceso de Relación con el Ciudadano o designado por el líder del Proceso.
El Proceso de Relación con el Ciudadano asistirá y participará en las capacitaciones brindadas por la Oficina de Tecnología de Información (OTI) cada vez que se programen y el enlace SIG socializar la información del	02/01/2026	31/12/2026	Enlace SIG del Proceso de Relación con el Ciudadano o designado por el líder del Proceso.

Plan de Acción	Fecha Inicio	Fecha Fin	Responsable
Sistema de Gestión de Seguridad de la Información a los funcionarios, contratistas y operadores del proceso cada vez que la Oficina de Tecnología de la Información (OTI) las publique. **Evidencia:** Correo electrónico replicados por el enlace del proceso para participar en las charlas de seguridad de la información, socialización de información del Sistema de Gestión de Seguridad de la Información y listas de asistencias a las charlas. **(A.6.3).**			

Tabla No.36 – Plan de acción establecido en la gestión de riesgos de Seguridad de la Información del proceso de Relación con el Ciudadano

8.1.13. Gestión Interinstitucional

En relación con el proceso de Gestión Interinstitucional se identificó un (1) riesgo con nivel de severidad residual "Moderado":

Redacción del riesgo	Nivel de Severidad Riesgo Inherente	Nivel de Severidad Riesgo Residual	Tratamiento	Comentario Tratamiento
Posibilidad de pérdida reputacional ante nuestras partes interesadas por falta de disponibilidad y mal uso de los activos de información críticos del proceso, debido a la falta de apropiación de las políticas y lineamientos de Seguridad de la Información.	**Moderado**	**Moderado**	Reducir - Mitigación	Se define fortalecer al control actual, con la definición de un Plan de Acción adicional con el fin de evitar su materialización.

Tabla No.37 – Riesgo identificado del proceso de Relación con el Ciudadano

Es importante mencionar que, el nivel de severidad residual se determinó teniendo en cuenta los siguientes controles existentes:

Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
El Proceso de Gestión Interinstitucional retroalimenta a los funcionarios y contratistas frente al reporte emitido por la Oficina de Tecnología de Información (OTI) sobre el estado de uso de OneDrive. **Evidencia:** Socialización del correo electrónico enviado por la OTI sobre el estado del uso de OneDrive de Proceso. **(A.5.16, A.8.2, A.8.3, A.8.13).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo

Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
El Proceso de Gestión Interinstitucional define la herramienta SharePoint para el almacenamiento de la información del proceso, por lo que cada vez que se requiera un permiso especifico de acceso se remitirá solicitud a la Oficina de Tecnología de Información (OTI) **Evidencia:** Correo de solicitud cada vez que se requiera el acceso. En caso de no tener solicitudes se deberá enviar correo por parte del líder del proceso indicando que en el periodo no se efectuó dicho requerimiento. **(A.5.16, A.8.2, A.8.3, A.8.13).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo
El Proceso de Gestión Interinstitucional implementa los protocolos de seguridad de la información definidos por la Oficina de Tecnología de la Información OTI, por lo que se diligenciará y enviará los acuerdos de confidencialidad para uso de sistemas y aplicativos de la UARIV cada vez que ingrese una persona contratista o servidora pública a la entidad. **Evidencia:** Documentos de acuerdo de confidencialidad debidamente firmados. **(A.5.16, A.8.2, A.8.3, A.8.13).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo

Tabla No.38 – Controles existentes identificados en la gestión de riesgos de Seguridad de la Información del proceso de Relación con el Ciudadano

Adicionalmente, el Proceso definió el siguiente plan de acción para el tratamiento del riesgo identificado:

Plan de Acción	Fecha Inicio	Fecha Fin	Responsable
"El Proceso de Gestión Interinstitucional asistirá y participará en las capacitaciones brindadas por la Oficina de Tecnología de Información (OTI), cada vez que se programen con el fin de dar cumplimiento a la implementación de la política del Sistema de Gestión de seguridad y privacidad de información, prevención de riesgos de seguridad digital y apropiación de conocimientos del SGSI. **Evidencia:** Correo electrónico con invitación a participar en las charlas de seguridad de la información, comunicación interna del material de seguridad generada por la Oficina de la Tecnología de la Información (OTI) y listas de asistencia. **(A.6.3).**	02/01/2026	31/12/2026	Enlace SIG del Proceso Gestión Interinstitucional o designado por el líder del Proceso.

Tabla No.39 – Plan de acción establecido en la gestión de riesgos de Seguridad de la Información del proceso de Relación con el Ciudadano

8.1.14. Prevención Urgente Atención Inmediatez

En relación con el proceso de Prevención Urgente Atención Inmediatez se identificó un (1) riesgo con nivel de severidad residual "Moderado":

Redacción del riesgo	Nivel de Severidad Riesgo Inherente	Nivel de Severidad Riesgo Residual	Tratamiento	Comentario Tratamiento
Posibilidad de pérdida económica y reputacional por pérdida de la Disponibilidad de la Información de la Entidad, debido a la falla o ausencia de controles de seguridad aplicables.	**Alto**	**Moderado**	Reducir - Mitigación	Se define planes de acción adicionales con el fin de evitar la materialización del riesgo.

Tabla No.40 – Riesgo identificado del proceso de Prevención Urgente Atención Inmediatez

Es importante mencionar que, el nivel de severidad residual se determinó teniendo en cuenta los siguientes controles existentes:

Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
El(la) Profesional designado(a) por el(la) líder del Proceso de Prevención Urgente y Atención en la Inmediatez deberá hacer seguimiento a la suscripción del ""Acuerdo de Confidencialidad"" con cada uno de los funcionarios, contratistas y/o operadores del Proceso, cuando se requiere acceder a los Sistemas de información y/o Servicios TI en las que se procesa y/o almacena la información de la Entidad. En caso de no contar con el ""Acuerdo"", no se asignará accesos ni usuarios; Es importante mencionar que los usuarios serán deshabilitados una vez expire la fecha de vigencia o cierre de periodo. Este control permite dar cumplimento a las políticas de seguridad de la información definidas por la entidad, por lo que es importante indicarles a los funcionarios, contratistas y/o operadores del Proceso las implicaciones que se pueden presentar por el uso inadecuado de la información en aras de obtener un beneficio económico por la atención y orientación a las víctimas. Evidencia: Los Acuerdos de Confidencialidad suscritos por el proceso de Proceso de Prevención Urgente y Atención en la Inmediatez y/o reporte de dicho registro. **(A.6.6).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo
El(la) Profesional designado(a) por el(la) líder del Proceso de Prevención Urgente y Atención en la Inmediatez deberá hacer seguimiento a la disponibilidad de la información, incluso si está es eliminada por equivocación. En ese sentido, se procederá a realizar procesos para la recuperación de la información de forma manual con el fin de tener la información disponible. **Evidencia:** Correos de gestión de la información que se está recuperando. En el caso de que en el periodo no se haya efectuado recuperación de información, se deberá enviar correo indicándole al líder de proceso que no se efectuó dicho requerimiento. **(A.5.1, A.5.2, A.5.3, A.5.4, A.5.10, A.5.11).**	Impacto	Correctivo	Manual	Sin Documentar	Con registro	Aleatorio

Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
El(la) Profesional designado(a) por el(la) líder del Proceso de Prevención Urgente y Atención en la Inmediatez deberá hacer seguimiento al acceso a las herramientas SharePoint para el almacenamiento de la información designado para la dependencia, por lo que cada vez que se requiera un permiso especifico de acceso se remitirá solicitud a la Oficina de Tecnología de Información (OTI). **Evidencia:** Correo de solicitud cada vez que se requiera el acceso. En caso de no tener solicitudes se deberá enviar correo por parte del líder del proceso indicando que en el periodo no se efectuó dicho requerimiento. **(A.5.16, A.8.2, A.8.3, A.8.13).**	Probabilidad	Preventivo	Automatizado	Documentado	Con registro	Continuo

Tabla No.41 – Controles existentes identificados en la gestión de riesgos de Seguridad de la Información del proceso de Prevención Urgente Atención Inmediatez

Adicionalmente, el Proceso definió el siguiente plan de acción para el tratamiento del riesgo identificado:

Plan de Acción	Fecha Inicio	Fecha Fin	Responsable
"El(la) Profesional designado(a) por el(la) líder del Proceso de Prevención Urgente y Atención en la Inmediatez deberá hacer seguimiento al acceso a las herramientas SharePoint para el almacenamiento de la información designado para la dependencia, por lo que cada vez que se requiera un permiso especifico de acceso se remitirá solicitud a la Oficina de Tecnología de Información (OTI). **Evidencia:** Correo de solicitud cada vez que se requiera el acceso. En caso de no tener solicitudes se deberá enviar correo por parte del líder del proceso indicando que en el periodo no se efectuó dicho requerimiento. **(A.5.16, A.8.2, A.8.3, A.8.13).**	02/01/2026	31/12/2026	Subdirección de Prevención y Atención de Emergencias y áreas adscritas.

Tabla No.42 – Plan de acción establecido en la gestión de riesgos de Seguridad de la Información del proceso de Prevención Urgente Atención Inmediatez

8.1.15. Gestión para la Asistencia

En relación con el proceso de Gestión para la Asistencia se identificaron dos (1) riesgos con nivel de severidad residual "Moderado":

Redacción del riesgo	Nivel de Severidad Riesgo Inherente	Nivel de Severidad Riesgo Residual	Tratamiento	Comentario Tratamiento
Posibilidad de pérdida económica y reputacional por pérdida de la Confidencialidad e integridad de la Información de la Entidad, debido a la falla o ausencia de controles relacionados con el acceso a información clasificada y/o reservada y el uso adecuado de la información	**Moderado**	**Moderado**	Reducir - Mitigación	Se define planes de acción adicionales con el fin de evitar la materialización del riesgo.

Tabla No.43 – Riesgo identificado del proceso de Gestión para la Asistencia

Es importante mencionar que, el nivel de severidad residual se determinó teniendo en cuenta los siguientes controles existentes:

Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
"El Proceso de Gestión para la Asistencia suscribe un ""Acuerdo de Confidencialidad"" con cada uno de los funcionarios y/o contratistas y/o operador del Proceso, cuando se requiere acceder a los Sistemas de información y/o Servicios TI en las que se procesa y/o almacena la información de la Entidad, en caso de NO contar con el ""Acuerdo"", no se asignara accesos, ni usuarios. En el caso de que se venza el ""Acuerdo"" el usuario será deshabilitado; Asimismo, el líder del Proceso de Gestión para la Asistencia establece los perfiles de acceso a los funcionarios, contratistas y/o operadores de acuerdo con las actividades a desarrollar. Este control permite dar cumplimento a las políticas de seguridad de la información definidas por la entidad, por lo que es importante indicarles a los funcionarios y/o contratistas y/o operadores del Proceso las implicaciones que se pueden presentar por el uso inadecuado de la información en aras de obtener un beneficio económico por la atención y orientación a las víctimas. Evidencia: Los Acuerdos de Confidencialidad suscritos por el proceso de Gestión para la asistencia y/o reporte de dicho registro. **(A.6.6, A.5.16, A.8.2, A.8.3, A.8.13).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo

Tabla No.44 – Controles existentes identificados en la gestión de riesgos de Seguridad de la Información del proceso de Gestión para la Asistencia

Adicionalmente, el Proceso definió el siguiente plan de acción para el tratamiento del riesgo identificado:

Plan de Acción	Fecha Inicio	Fecha Fin	Responsable
El enlace SIG del Proceso de Gestión para la Asistencia socializa la información del Sistema de Gestión de Seguridad de la Información a los funcionarios, contratistas y operadores del proceso cada vez que la Oficina de Tecnología de la Información (OTI) las publique ó se identifique la necesidad al interior del proceso. **Evidencia:** Correo electrónico de socialización de información del Sistema de Gestión de Seguridad de la Información. **(A.6.3).**	02/01/2026	31/12/2026	Enlace SIG de Gestión para la Asistencia o designado por el líder del Proceso.

Plan de Acción	Fecha Inicio	Fecha Fin	Responsable
El Proceso de Gestión para la Asistencia define la herramienta SharePoint para el almacenamiento de la información del proceso, por lo que cada vez que se requiera un permiso especifico de acceso se remitirá solicitud a la Oficina de Tecnología de Información (OTI) **Evidencia:** Correo de solicitud cada vez que se requiera el acceso. En caso de no tener solicitudes se deberá enviar correo indicando que en el periodo no se efectuó dicho requerimiento. **(A.5.16, A.8.2, A.8.3, A.8.13).**	02/01/2026	31/12/2026	Enlace SIG de Gestión para la Asistencia o designado por el líder del Proceso.

Tabla No.45 – Plan de acción establecido en la gestión de riesgos de Seguridad de la Información del proceso de Gestión para la Asistencia

8.1.16. Participación y Visibilización

En relación con el proceso de Participación y Visibilización se identificó un (1) riesgo con nivel de severidad residual "Moderado":

Redacción del riesgo	Nivel de Severidad Riesgo Inherente	Nivel de Severidad Riesgo Residual	Tratamiento	Comentario Tratamiento
Posibilidad de pérdida económica y reputacional por perdida de disponibilidad, integridad y confidencialidad de la información, debido a la omisión, ausencia o insuficiencia de seguimiento a los controles, lineamientos y procedimientos del proceso de Participación y visibilización, para la protección y acceso controlado a la información clasificada y/o reservada.	**Alto**	**Moderado**	Reducir - Mitigación	Se define planes de acción adicionales con el fin de evitar la materialización del riesgo.

Tabla No.46 – Riesgo identificado del proceso de Participación y Visibilización

Es importante mencionar que, el nivel de severidad residual se determinó teniendo en cuenta los siguientes controles existentes:

Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
El/la enlace SIG-SI informa a los funcionarios y contratistas del proceso de Participación y visibilización frente al reporte emitido por la Oficina de Tecnología de Información (OTI) sobre el estado de uso del SharePoint de la Subdirección de Participación y el OneDrive. **Evidencia:** Correo electrónico enviado por el/la enlace SIG-SI con el reporte de uso del SharePoint y OneDrive. **(A.5.16, A.8.2, A.8.3, A.8.13).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo

Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
Los colaboradores suscriben un ""Acuerdo de Confidencialidad"" cuando se requiere acceder a los Sistemas de información y/o Servicios TI en los que se procesa y/o almacena la información de la Entidad. El ""Acuerdo"" es un requisito para la asignación de usuario con el dominio institucional en la plataforma de Microsoft 365, en caso en que se venza el ""Acuerdo"" el usuario será deshabilitado. **Evidencia:** Acuerdo de Confidencialidad suscritos por los colaboradores del proceso de Proceso de Participación y visibilización y/o correo de solicitud a la OTI de des habilitación de usuarios inactivos y/o correo a la OTI con solicitud de permisos asociados al SharePoint de la Subdirección de Participación. **(A.6.6).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo
El/la enlace del SIG-SI realiza la verificación de la transferencia de los activos de información según la TRD con las propiedades de integridad, confidencialidad y disponibilidad, desde el OneDrive de los colaboradores al SharePoint de la Subdirección de Participación como único repositorio del proceso. **Evidencia:** Correo con informe entregado al subdirector/a de Participación con el estado de los activos de información según la TRD ubicados en el SharePoint de la Subdirección de Participación. **(A.5.2, A.5.3, A.5.15).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo

Tabla No.47 – Controles existentes identificados en la gestión de riesgos de Seguridad de la Información del proceso de Participación y Visibilización

Adicionalmente, el Proceso definió el siguiente plan de acción para el tratamiento del riesgo identificado:

Plan de Acción	Fecha Inicio	Fecha Fin	Responsable
Los colaboradores del Proceso de Participación y visibilización participan en las capacitaciones brindadas por la Oficina de Tecnología de Información (OTI), para dar cumplimiento a la implementación de la política del Sistema de Gestión de seguridad y privacidad de información, prevención de riesgos de seguridad digital y apropiación de conocimientos del SGI-SI. **Evidencia:** Correo electrónico del enlace SIG-SI recordando, invitando y motivando a los colaboradores a participar en las charlas, capacitaciones lideradas por la OTI y/o recomendaciones de seguridad de la información y/o socialización a los colaboradores con el informe del estado de los activos de información según la TRD ubicados en el SharePoint de la Subdirección de Participación. **(A.6.3).**	01/01/2026	31/12/2026	Enlace SIG-SI del Proceso Participación y Visibilización o designado por el líder del Proceso.

Tabla No.48 – Plan de acción establecido en la gestión de riesgos de Seguridad de la Información del proceso de Participación y Visibilización

8.1.17. Gestión de Información

En relación con el proceso de Gestión de Gestión de Información se identificaron diez (10) riesgos, categorizados por dependencia (Oficina de TI y Subdirección Red Nacional de Información). Para los riesgos relacionados con la Oficina de TI se incluye el Dominio específico, de la siguiente manera:

Dependencia / Dominio	Redacción del riesgo	Nivel de Severidad Riesgo Inherente	Nivel de Severidad Riesgo Residual	Tratamiento	Comentario Tratamiento
Oficina de TI Infraestructura TI	Posibilidad de pérdida económica y reputacional por pérdida de la Disponibilidad de la Información de la Entidad, debido a la falla o ausencia de controles de seguridad aplicables para la implementación de políticas de backups, gestión de identidades, control de acceso a los recursos y/o repositorios de la información.	**Extremo**	**Extremo**	Reducir - Mitigación	Se define planes de acción adicionales con el fin de evitar la materialización del riesgo.
Oficina de TI Sistemas de Información	Posibilidad de pérdida económica y reputacional por pérdida a la Integridad y disponibilidad de la Información de la Entidad, debido a la falla o ausencia de controles de seguridad aplicables para el acceso a los recursos, uso adecuado de la información y la ejecución del control de cambios de (nuevos desarrollos y/o actualizaciones).	**Alto**	**Alto**	Reducir - Mitigación	Se define planes de acción adicionales con el fin de evitar la materialización del riesgo.
Oficina de TI Servicios TI	Posibilidad de pérdida económica y reputacional por pérdida de la Confidencialidad de la Información de la Entidad, debido a la falla o ausencia de controles relacionados con el acceso a información clasificada y/o reservada.	**Alto**	**Alto**	Reducir - Mitigación	Se define planes de acción adicionales con el fin de evitar la materialización del riesgo.
Oficina de TI Arquitectura Empresarial	Posibilidad de pérdida económica y reputacional por pérdida de la Disponibilidad de la Información de la Entidad, debido a la falla o ausencia de controles de seguridad aplicables que permiten dar cumplimiento a las políticas y lineamientos relacionados con los principios de Arquitectura Empresarial.	**Moderado**	**Moderado**	Reducir - Mitigación	Se define planes de acción adicionales con el fin de evitar la materialización del riesgo.
Seguridad de la Información	Posibilidad de pérdida económica y reputacional por pérdida de la Disponibilidad de la Información de la Entidad, debido a las fallas en la identificación y seguimiento de los riesgos de Seguridad y desactualización del Inventario de Activos de Información de la Entidad.	**Alto**	**Alto**	Reducir - Mitigación	Se define planes de acción adicionales con el fin de evitar la materialización del riesgo.
	Posibilidad de pérdida económica y reputacional por pérdida a la Integridad y Disponibilidad de la Información de la Entidad, debido a la falla o ausencia de controles	**Extremo**	**Alto**	Reducir - Mitigación	Se define planes de acción adicionales con el fin de evitar la materialización del riesgo.

Dependencia / Dominio	Redacción del riesgo	Nivel de Severidad Riesgo Inherente	Nivel de Severidad Riesgo Residual	Tratamiento	Comentario Tratamiento
	para la remediación de vulnerabilidades en la Infraestructura Tecnológica y/o materialización de incidentes de seguridad.				
Subdirección RNI	Posibilidad de pérdida reputacional por la indisponibilidad de fuentes, bases de datos de información y/o sistemas de información de la población víctima de acuerdo con la necesidad, en las herramientas, aplicativos y visores utilizados por la SRNI, debido a que las entidades limitan el intercambio de información bajo argumentos políticos legales o voluntades personales, la falta de infraestructura tecnológica adecuada y disponible, el incumplimiento por parte de las entidades externas receptoras de la información, de los acuerdos y/o convenios de intercambio de información firmados con la Unidad, o porque la información de los sistemas de información internos tienen deficiencias en la calidad de los datos que se generan y que se utiliza como insumo para la gestión.	**Moderado**	**Moderado**	Aceptar	Se define establecer plan de acción para mitigar y/o reducir el nivel y para atender las causas por las que se puede presentar el riesgo, atendiendo lo establecido en la metodología de administración del riesgo.
	Posibilidad de pérdida reputacional por divulgación o alteración no autorizada de información, con ocasión a la pérdida o hurto de esta, debido al extravío o hurto del dispositivo en campo o herramientas donde se está tomando la encuesta en el esquema de acompañamiento presencial del levantamiento de información a través de entrevista de caracterización.	**Bajo**	**Bajo**	Reducir - Mitigación	Dado el nivel de severidad residual del riesgo no se hace necesario implementar un plan de acción.
	Posibilidad de pérdida reputacional por acceso no autorizado a las herramientas tecnológicas de la SRNI por captura, procesamiento y/o uso inadecuado de la información de identificación personal recopilada sobre los datos de la población víctima, debido al uso indebido de la información de Identificación Personal con propósitos desconocidos o ilegales.	**Moderado**	**Bajo**	Aceptar	Dado el nivel de severidad residual del riesgo no se hace necesario implementar un plan de acción.
	Posibilidad de pérdida de confidencialidad por el uso indebido de la información dispuesta por la SRNI, ocasionado por un alto nivel de consultas en el aplicativo de VIVANTO para el módulo de consulta individual.	**Bajo**	**Bajo**	Aceptar	Dado el nivel de severidad residual del riesgo no se hace necesario implementar un plan de acción.

Tabla No.49 – Riesgo identificado del proceso de Gestión de Información

Unidad para las Víctimas

Es importante mencionar que, el nivel de severidad residual se determinó teniendo en cuenta los siguientes controles existentes:

Dominio	Redacción del riesgo	Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
Oficina de TI Infraestructura TI	Posibilidad de pérdida económica y reputacional por pérdida de la Disponibilidad de la Información de la Entidad, debido a la falla o ausencia de controles de seguridad aplicables para la implementación de políticas de backups, gestión de identidades, control de acceso a los recursos y/o repositorios de la información.	El proceso de Gestión de la Información, en cabeza del Dominio de Infraestructura TI, realiza ejecución de las copias de seguridad de las bases de datos de acuerdo con los lineamientos establecidos **Evidencia:** Reporte donde se observa los backups y/o logs de ejecución de las copias de seguridad de base de datos realizadas en el periodo por el del Dominio de Infraestructura TI. **(A.8.13).**	Probabilidad	Preventivo	Automatizado	Documentado	Con registro	Continuo
		"El proceso de Gestión de la Información, en cabeza del Dominio de Infraestructura TI realiza la ejecución de las copias de seguridad a servidores y dispositivos de res de acuerdo con la periodicidad establecida. **Evidencia:** Reporte donde se evidencias las copias de seguridad ejecutadas por el del Dominio de Infraestructura TI. **(A.8.13).**	Probabilidad	Preventivo	Automatizado	Documentado	Con registro	Continuo
		El proceso de Gestión de la Información, en cabeza del Dominio de Infraestructura TI, aplica controles de acceso a los usuarios de cada proceso para (consulta, adición y modificación) de la información en la herramienta de SharePoint de la Entidad. **Evidencia:** Correo de solicitud de los procesos para conceder los permisos asociados al repositorio de SharePoint en el periodo y/o correo del líder del Dominio que indique que para el presente periodo no se recibieron solicitudes de accesos. **(A.5.2, A.5.3, A.5.15).**	Probabilidad	Preventivo	Automatizado	Documentado	Con registro	Continuo
Oficina de TI Sistemas de Información	Posibilidad de pérdida económica y reputacional por pérdida a la Integridad y disponibilidad de la Información de la Entidad, debido a la falla o ausencia de controles de seguridad aplicables para el acceso a los recursos, uso adecuado de la información y la ejecución del control de cambios de (nuevos	El proceso de Gestión de la Información desde el Dominio de Sistemas de Información, registra los backlogs en Azure Devops con el fin de llevar un control de los nuevos desarrollos y/o actualizaciones de los sistemas de información que fueron aceptados y aprobados. **Evidencia:** Pantallazo del registro de los backlogs en Azure Devops efectuados en el periodo y/o correo del líder del Dominio que indique que para el presente periodo no se realizaron desarrollos nuevos o actualizaciones. **(A.8.14).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo

Dominio	Redacción del riesgo	Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
	desarrollos y/o actualizaciones).	El proceso de Gestión de la Información desde el Dominio de Sistemas de Información, realizan la verificación de controles aplicables que son requisitos de seguridad en el ciclo de vida de desarrollo de software para los nuevos desarrollos y/o actualizaciones. **Evidencia:** Archivo de verificación de los controles de seguridad y/o Pantallazo del archivo del registro de verificación de los controles de seguridad en Azure Devops y/o correo del líder del Dominio que indique que para el presente periodo no se realizaron desarrollos nuevos o actualizaciones. **(A.8.25, A.8.26).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo
		El proceso de Gestión de la Información desde el Dominio de Seguridad de la información implementa el protocolo de gestión de control de cambios para los desarrollos nuevos y/o actualizaciones de los sistemas de información. **Evidencia:** Registro de formato de cambios y/o acta de comité de control de cambios aprobados y/o rechazados y/o correo del líder del Dominio que indique que para el presente periodo no se presentaron controles de cambios par desarrollos nuevos o actualizaciones. **(A.8.32).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo
Oficina de TI Servicios TI	Posibilidad de pérdida económica y reputacional por pérdida de la Confidencialidad de la Información de la Entidad, debido a la falla o ausencia de controles relacionados con el acceso a información clasificada y/o reservada.	El proceso de Gestión de la Información, en cabeza del Dominio de Servicios TI, suscribe un ""Acuerdo de Confidencialidad"" con cada uno de los funcionarios y/o contratistas Y/o Operadores del Proceso cuando se requiere acceder a los Sistemas de información y/o Servicios TI en las que se procesa y/o almacena la información de la Entidad, en caso de contar con el ""Acuerdo"", no se asignará accesos ni usuarios; para el caso de que se venza el ""Acuerdo"" el usuario será deshabilitado. Este control permite dar cumplimento a las políticas de seguridad de la información definidas por la entidad, por lo que es importante indicarles a los funcionarios y/o contratistas y/o operadores del Proceso las implicaciones que se pueden presentar por el uso inadecuado de la información en aras de obtener un beneficio económico por la atención y orientación a las víctimas. **Evidencia:** Los Acuerdos de Confidencialidad suscritos por el Dominio de Servicios TI y/o correo del líder del dominio que indique que para el presente periodo no se suscribieron Acuerdos de Confidencialidad. **(A.6.6).**	Probabilidad	Preventivo	Manual	Documentado	Sin registro	Continuo

Dominio	Redacción del riesgo	Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
		El proceso de Gestión de la Información, en cabeza del Dominio de Servicios TI, realiza la segregación de tareas en la atención o ejecución del soporte técnico solicitado a través de la Mesa de Servicios Tecnológicos. **Evidencia:** Segregación de tareas en la herramienta de gestión ""ARANDA"". **(A 5.2, A.5.3, A.5.4).**	Probabilidad	Preventivo	Automatizado	Documentado	Con registro	Continuo
		El proceso de Gestión de la Información, en cabeza del Dominio de Servicios TI, realiza reporte en la herramienta de gestión ""ARANDA"" para la creación o inactivación de usuarios (funcionario, contratista u operador) del Dominio Servicios TI. **Evidencia:** Registro de los casos reportados para la creación o inactivación de usuario en la herramienta de gestión ""ARANDA"". **(A.5.15, A.5.16, A.5.17, A.5.18, 8.3, 8.26).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo
Oficina de TI Arquitectura Empresarial	Posibilidad de pérdida económica y reputacional por pérdida de la Disponibilidad de la Información de la Entidad, debido a la falla o ausencia de controles de seguridad aplicables que permiten dar cumplimiento a las políticas y lineamientos relacionados con los principios de Arquitectura Empresarial.	El Proceso de Gestión de la Información desde el Dominio de Estrategia y Gobierno, realiza la revisión, actualización y seguimiento del Plan Estratégico de Tecnología de la Información (PETI) con el fin de que este integre y cumplan con los proyectos definidos en el Plan Estratégico de Seguridad de la Información (PESI) de acuerdo con los lineamientos del Gobierno Nacional. **Evidencia:** Acta de las mesas de trabajo para la actualización del PETI y/o acta de seguimiento del PETI. **(A 5.1, A.5.2, A.5.8, A.5.36).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo
		El Proceso de Gestión de la Información desde el Dominio de Arquitectura Empresarial, realiza la revisión Del Documento de Arquitectura de Referencia de la Entidad. **Evidencia:** Acta de revisión y/o documento actualizado de Arquitectura de Referencia de la Entidad. **(A.5.36).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo

Dominio	Redacción del riesgo	Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
Seguridad de la Información	Posibilidad de pérdida económica y reputacional por pérdida de la Disponibilidad de la Información de la Entidad, debido a las fallas en la identificación y seguimiento de los riesgos de Seguridad y desactualización del Inventario de Activos de Información de la Entidad.	El proceso de Gestión de la Información, desde el Dominio de Seguridad, realiza seguimiento y gestión con cada uno de los Procesos del Nivel Central y Dirección Territorial la actualización periódica del Inventario de Activos de Información de la Entidad y la matriz de riesgos por proceso. **Evidencia:** Correo de programación de mesas de trabajo para actualización del Inventario y/o Inventario de Activos actualizados de los Procesos y Direcciones Territoriales. Matriz de riesgos de seguridad de la información consolidada. **(A.5.9).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo
		El proceso de Gestión de la Información, desde el Dominio de Seguridad, realiza la presentación para aprobación de los Activos de Información, los Instrumentos de Gestión Pública y el Plan de tratamiento de riesgos ante el Comité Institucional de Gestión y Desempeño de la Entidad. **Evidencia:** Presentación de los Activos de Información y Plan de tratamiento de riesgos al Comité Institucional de Gestión y Desempeño y/o acta de aprobación de los Instrumentos de Gestión de Información Pública. **(A.5.9).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo
	Posibilidad de pérdida económica y reputacional por pérdida a la Integridad y Disponibilidad de la Información de la Entidad, debido a la falla o ausencia de controles para la remediación de vulnerabilidades en la Infraestructura Tecnológica y/o materialización de incidentes de seguridad.	El proceso de Gestión de la Información, desde el Dominio de Seguridad, realiza de manera semestral el análisis de vulnerabilidades a Sistemas de Información y Servicios TI de la Entidad. **Evidencia:** Reporte de análisis de vulnerabilidades a Sistemas de Información y Servicios TI semestral. **(A.8.8).**	Probabilidad	Preventivo	Automatizado	Documentado	Con registro	Continuo
		El proceso de Gestión de la Información, desde el Dominio de Seguridad, realizará mesas de trabajo con los responsables de cada Servicios TI con el fin de establecer las actividades, fechas y responsables de las remediaciones de las vulnerabilidades identificadas en la Infraestructura Tecnológica y sistemas de información de la Entidad. **Evidencia:** Seguimiento al Plan de remediaciones de vulnerabilidades identificadas en el mes. **(A.8.8, A.8.12).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo

Dominio	Redacción del riesgo	Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
		El proceso de Gestión de la Información, en cabeza del Dominio de Seguridad, en el marco del cumplimiento del Procedimiento de Incidentes de Seguridad realizará la gestión a los incidentes reportados en la herramienta de gestión ""ARANDA"" los cuales deberán estar documentados como base de conocimiento que permitan dar solución a futuros eventos de seguridad. **Evidencia:** Reportes de casos mensuales en Aranda. **(A.5.24, A.5.25, A.5.26, A.5.27, A.5.28).**	Impacto	Correctivo	Manual	Documentado	Con registro	Continuo
Subdirección RNI	Posibilidad de pérdida reputacional por la indisponibilidad de fuentes, bases de datos de información y/o sistemas de información de la población víctima de acuerdo con la necesidad, en las herramientas, aplicativos y visores utilizados por la SRNI, debido a que las entidades limitan el intercambio de información bajo argumentos políticos legales o voluntades personales, la falta de infraestructura tecnológica adecuada y disponible, el incumplimiento por parte de las entidades externas receptoras de la información, de los acuerdos y/o convenios de intercambio de información firmados con la Unidad, o porque la información de los sistemas de información internos tienen deficiencias en la calidad de los datos que se generan y que se utiliza	El líder o apoyo del procedimiento de Articulación interinstitucional y dinamización de la información AIDI, realiza por demanda la oficialización del acuerdo de intercambio de información, generando un anexo técnico al anterior documento donde se encuentran las reglas que rigen el intercambio, acompañado del diccionario de datos, que es el insumo para el entendimiento de la fuente; para las entidades que no aplican documento técnico esta información queda en un oficio, correo electrónico o acta. De igual manera se realiza un seguimiento a lo estipulado en el documento técnico a través del oficio, correos electrónicos o actas de reunión. **Evidencia:** Anexo técnico, oficio, correo electrónico o acta. En caso de que la solicitud no tenga acuerdo o este incompleta, no se realizara el cargue de información a los sistemas de la SRNI. **(A.5.14).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo
		El líder o apoyo de los procedimientos de la Subdirección Red Nacional de Información-SRNI, cada vez que se requiera, solicita a través de correo electrónico o acta de reunión a la Oficina de Tecnologías de Información o al personal encargado de la actividad la ampliación del recurso tecnológico, con el fin de soportar las nuevas necesidades en el intercambio de información. En caso de no recibir respuesta por parte del personal encargado se programa reunión con los jefes de las áreas técnicas para definir los alcances y motivos de la demora en la respuesta. **Evidencia:** Correo electrónico o Acta de reunión. **(A.8.6).**	Probabilidad	Detectivo	Manual	Documentado	Con registro	Continuo

Dominio	Redacción del riesgo	Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
	como insumo para la gestión.	El líder o apoyo del Procedimiento de Articulación interinstitucional y dinamización de la información-AIDI, cada vez que se realiza el corte de las fuentes verifica el cumplimiento de lo establecido en los acuerdos y/o convenios entre la Unidad y las Entidades Nacionales, a través de los cortes dispuestos en la herramienta Vivanto contra lo establecido en los acuerdos de intercambio, con el objetivo de garantizar la información actualizada que dé cuenta de los datos asociados a la población víctima. En caso de incumplimiento, se notifica a la entidad respectiva. **Evidencia:** Correo electrónico, acta u oficio. **(A.5.14)**	Probabilidad	Detectivo	Manual	Documentado	Con registro	Continuo
		El líder o apoyo del procedimiento de Instrumentalización, cada vez que reciba una fuente, realiza una validación de esta en particular para las mediciones de Subsistencia Mínima, Superación de Situación de Vulnerabilidad e Indicadores de Goce Efectivo de Derechos, de acuerdo con las variables mínimas requeridas con el fin de validar la consistencia de variables a intercambiar con la entidad o área misional que se tiene el intercambio. En caso de inconsistencias se devuelve la fuente solicitando aclaraciones. **Evidencia:** el soporte es la aprobación del metadato en el inventario de fuentes y/o correo electrónico del cargue en Vivanto. **(A.5.14)**	Probabilidad	Detectivo	Manual	Documentado	Con registro	Continuo
	Posibilidad de pérdida reputacional por divulgación o alteración no autorizada de información, con ocasión a la pérdida o hurto de esta, debido al extravío o hurto del dispositivo en campo o herramientas donde se está tomando la encuesta en el esquema de acompañamiento presencial del levantamiento de información a través de entrevista de caracterización.	El apoyo técnico de la SRNI, cuando se requiera, realiza la asignación y configuración de los dispositivos que son propiedad de la SRNI cuando así se requiera. Como medida de seguridad, dichos dispositivos son protegidos mediante bloqueo por contraseña, la cual permite reactivar el equipo tras un período de inactividad. Esta acción se complementa con el cifrado de la memoria interna, cuya clave permanece exclusivamente bajo custodia de la SRNI. Adicionalmente, se lleva un control sobre la asignación y salida de los dispositivos, garantizando su trazabilidad y uso autorizado. **Evidencia:** Correo para el control de asignación y salida de los dispositivos de la Entidad y screenshot. **(A.5.3, A.5.16, A.8.2).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo

Dominio	Redacción del riesgo	Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
		El apoyo o líder del procedimiento de la Estrategia de Caracterización cuando se requiera articula la implementación de la caracterización con las mesas de víctimas y demás actores del territorio. En caso de no contar con la solicitud no se podrá atender el requerimiento. **Evidencia:** como evidencia se tiene actas de reuniones, convenios interinstitucionales, oficios o correos electrónicos. **(A.6.3)**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo
		El colaborador del procedimiento de la Estrategia de Caracterización socializa y capacita el manejo de herramientas tecnológicas y aplicativo al personal que realiza el levantamiento de información (presencial y no presencial), cada vez que la entidad solicita acompañamiento. En caso de no ser viable su ejecución, no se podrá activar usuarios para el levantamiento de información. **Evidencia:** Acta de reunión, listas de asistencia, oficios o correos electrónicos de la capacitación. **(A.6.3).**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo
		El apoyo o líder de la mesa de servicios de la SRNI, cuando se requiera inactiva los usuarios del módulo de caracterización (versión WEB y OFFLINE) de la siguiente forma: 1. Los usuarios se inactivan de acuerdo con su periodo de vinculación contractual. 2. El primero de enero de cada vigencia se inactivan todos los accesos a Vivanto. 3. Bloqueo automático por no registrar actividad del usuario en un periodo de 30 días calendario. 4. A solicitud de las entidades externas o cliente interno. 5. En caso de detectar mal uso de la herramienta se inactivará el usuario. Evidencia: Registro en ARANDA por solicitud de inactivación y/o correo de solicitud de inactivación de usuarios. **(A.5.3, A.5.16, A.8.2, A.5.17, A.5.18).**	Impacto	Correctivo	Manual	Documentado	Con registro	Continuo

Dominio	Redacción del riesgo	Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
	Posibilidad de pérdida reputacional por acceso no autorizado a las herramientas tecnológicas de la SRNI por captura, procesamiento y/o uso inadecuado de la información de identificación personal recopilada sobre los datos de la población víctima, debido al uso indebido de la información de Identificación Personal con propósitos desconocidos o ilegales.	Cada vez que se contrata a un colaborador el subdirector de la Red Nacional de Información condiciona a los colaboradores encargados del procesamiento de Identificación Personal a ejecutar sus actividades previas a la suscripción de un acuerdo de confidencialidad que garantice el compromiso ético de utilizar la información en debida forma. En caso de no de no firmar el acuerdo de confidencialidad no se podrá procesar Información. **Evidencia:** Acuerdo de confidencialidad firmado por el Colaborador y supervisor. **(A.6.6)**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo
		Los encuestadores de la estrategia de caracterización, cada vez que se requiera, deben remitir la trazabilidad de la transmisión de la Identificación de Información Personal (IIP), garantizando el encripta miento de los datos para su adecuada disposición en el servidor. En caso de que el encuestador no remita dicha trazabilidad, se procede a verificar la información directamente en los dispositivos. El líder del procedimiento de caracterización solicita entonces al encuestador que, desde su usuario, transmita la información correspondiente y envíe un correo electrónico con la captura de pantalla que evidencie la transmisión de las entrevistas de caracterización. **Evidencia:** Correo con captura de pantalla de la transmisión de las entrevistas de caracterización tomadas a partir de los dispositivos offline. **(A.8.15).**	Probabilidad	Preventivo	Automatizado	Documentado	Con registro	Continuo
		El apoyo de seguridad de la información de la Subdirección Red Nacional de Información (SRNI), generar mensualmente revisiones internas a las consultas realizadas al módulo de consulta individual en el aplicativo Portal VIVANTO. **Evidencia:** Correo de alerta sobre la revisión mensual al módulo de consulta individual. **(A.5.15, A.5.33, A.8.34).**	Probabilidad	Preventivo	Manual	Sin Documentar	Con registro	Aleatorio
	Posibilidad de pérdida de confidencialidad por el uso indebido de la información dispuesta por la SRNI, ocasionado por un alto nivel de consultas en el aplicativo de VIVANTO para el módulo de consulta individual.	El apoyo de seguridad de la información de la Subdirección Red Nacional de Información (SRNI), genera mensualmente revisiones internas a las consultas realizadas al módulo de consulta individual en el aplicativo Portal VIVANTO. **Evidencia:** Correo de alerta sobre la revisión mensual al módulo de consulta individual. **(A.5.15, A.5.33, A.8.34)**	Probabilidad	Preventivo	Manual	Sin Documentar	Con registro	Aleatorio

Dominio	Redacción del riesgo	Descripción del control	Afectación del control	Tipo de Control	Implementación	Documentación	Evidencia	Frecuencia
		El apoyo de seguridad de la información de la Subdirección Red Nacional de Información (SRNI) realiza socializaciones sobre el uso adecuado de la información dispuesta en el aplicativo Portal VIVANTO. **Evidencia:** Socialización del uso adecuado. **(A.6.3)**	Probabilidad	Preventivo	Manual	Documentado	Con registro	Continuo
		La mesa de servicios de la Subdirección Red Nacional de Información (SRNI), inactiva los usuarios cuando se evidencien consultas elevadas en el mes inmediatamente anterior. **Evidencias:** Soporte de inactivación de usuarios por consultas elevadas en el mes. **(A.5.15, A.5.16, A.5.17, A.5.18, 8.3, 8.26).**	Impacto	Correctivo	Manual	Documentado	Con registro	Aleatorio

Tabla No.50 – Controles existentes identificados en la gestión de riesgos de Seguridad de la Información del proceso de Gestión de Información

Adicionalmente, el Proceso definió el siguiente plan de acción para el tratamiento del riesgo identificado:

Dominio	Plan de Acción	Fecha Inicio	Fecha Fin	Responsable
Oficina de TI Infraestructura TI	El proceso de Gestión de la Información, en cabeza del Dominio de Infraestructura TI, realizará pruebas de restauración Backup. **Evidencia:** Reporte donde se observa la restauración de backups ejecutados en el periodo el Dominio de Infraestructura TI. **(A.8.13).**	02/01/2026	31/12/2026	Dominio de Infraestructura TI de la OTI o designado por el líder del Proceso.
	El proceso de Gestión de la Información, en cabeza del Dominio de Infraestructura TI, atiende los casos reportados en la herramienta de gestion ""ARANDA"" para la creación o inactivación de de usuarios (funcionario, contratista u operador) de la Entidad. **Evidencia:** Registro de los casos reportados y atendidos en la herramienta de gestión ""ARANDA"" por Dominio de Infraestructura TI. **(A.5.15, A.5.16, A.5.17, A.5.18, 8.3, 8.26).**	02/01/2026	31/12/2026	Dominio de Infraestructura TI de la OTI o designado por el líder del Proceso.

Dominio	Plan de Acción	Fecha Inicio	Fecha Fin	Responsable
	El proceso de Gestión de la Información, en cabeza del Dominio de Infraestructura TI, realiza la gestión y seguimiento del mantenimiento preventivo de los dispositivos de red del Nivel Territorial de la Entidad ejecutado por el operador. **Evidencia:** Programación y seguimiento del mantenimiento preventivo y correctivo y/o correo del líder del dominio que indique que para el presente periodo no se realizó mantenimiento preventivo y/o correctivo. **(A.5.15, A.5.16, A.8.2).** (Emma)	02/01/2026	31/12/2026	Dominio de Infraestructura TI de la OTI o designado por el líder del Proceso.
Oficina de TI Sistemas de Información	"El Dominio de Sistemas de Información del Proceso de Sistemas de Información, asistirá y participará en las capacitaciones del Sistema de Gestión de Seguridad de la Información SGSI, brindadas por la Oficina de Tecnología de Información (OTI) cada vez que se programen. **Evidencia:** Lista de asistencia de las charlas de seguridad de la información donde se evidencia la participación de los Colaboradores del Dominio de Sistemas de Información. **(A.6.3).**	02/01/2026	31/12/2026	Dominio de Sistemas de información de la OTI o designado por el líder del Proceso.
Oficina de TI Servicios TI	El Proceso de Gestión de la Información desde el Dominio de Servicios TI, asistirá y participará en las capacitaciones del Sistema de Gestión de Seguridad de la Información SGSI, brindadas por la Oficina de Tecnología de Información (OTI) cada vez que se programen. **Evidencia:** Lista de asistencia de las charlas de seguridad de la información donde se evidencia la participación de los Colaboradores del Dominio de Sistemas de Información. **(A.6.3).**	02/01/2026	31/12/2026	Dominio de Servicios TI de la OTI o designado por el líder del Proceso.
Oficina de TI Arquitectura Empresarial	El Proceso de Gestión de la Información desde el Dominio de Arquitectura Empresarial, estructuro y utiliza el repositorio Arquitectura Empresarial en atención a los lineamientos de Mintic. **Evidencia:** Pantallazo del repositorio definido. **(A.5.16, A.8.2, A.8.3, A.8.13).**	02/01/2026	31/12/2026	Domino de Arquitectura Empresarial de la OTI o designado por el líder del Proceso.
	"El Proceso de Gestión de la Información desde el Dominio de Arquitectura Empresarial, asistirá y	02/01/2026	31/12/2026	Domino de Arquitectura Empresarial de la OTI o

Dominio	Plan de Acción	Fecha Inicio	Fecha Fin	Responsable
	participará en las capacitaciones del Sistema de Gestión de Seguridad de la Información SGSI, brindadas por la Oficina de Tecnología de Información (OTI) cada vez que se programen. **Evidencia:** Lista de asistencia de las charlas de seguridad de la información donde se evidencia la participación de los Colaboradores del Dominio de Arquitectura Empresarial. **(A.6.3).**			designado por el líder del Proceso.
Seguridad de la Información	El proceso de Gestión de la Información, desde el Dominio de Seguridad, realiza seguimiento y gestión para aumentar el porcentaje de cumplimiento del Instrumento del Modelo de Seguridad y Privacidad de la Información (MSPI). **Evidencia:** Instrumento del Modelo de Seguridad y Privacidad de la Información (MSPI). **(A.5.36).**	02/01/2026	31/12/2026	Domino de Seguridad de la Información de la OTI o designado por el líder del Proceso.
	El proceso de Gestión de la Información, desde el Dominio de Seguridad, definirá un Plan de Cultura y Sensibilización en Seguridad de la Información y realizará seguimiento de las actividades definidas. **Evidencia:** Plan de Cultura aprobado y/o seguimiento de las actividades definidas y desarrolladas mensualmente. **(A.6.3).**	02/01/2026	31/12/2026	Domino de Seguridad de la Información de la OTI o designado por el líder del Proceso.
	El proceso de Gestión de la Información, desde el Dominio de Seguridad, realizará revisión de la configuración de las herramientas de seguridad con el fin de verificar la aplicación de la política de restricción para el uso de medios de almacenamiento de información (USB) implementada en la Entidad. **Evidencia:** Pantallazos de la configuración de la política de restricción para el uso de medios de almacenamiento de información (USB) a diez (10) usuarios aleatorios de forma mensual. **(A.8.9).**	02/01/2026	31/12/2026	Domino de Seguridad de la Información de la OTI o designado por el líder del Proceso.

Dominio	Plan de Acción	Fecha Inicio	Fecha Fin	Responsable
	El proceso de Gestión de la Información, desde el Dominio de Seguridad, realizará la verificación del registro y/o sincronización, en la consola de antivirus o aseguramiento, de los equipos de propiedad de la Entidad. **Evidencia:** Registro mensual de la consola de los equipos que se sincroniza. **(A.8.20, A.8.21).**	02/01/2026	31/12/2026	Domino de Seguridad de la Información de la OTI o designado por el líder del Proceso.
Subdirección RNI	Realizar el seguimiento y reporte trimestral de la calidad de datos de las fuentes de información aprobadas y cargadas en el inventario de fuentes del módulo de Vivanto.	01/04/2026	31/12/2026	Lideres de Procedimientos de Instrumentalización y AIDI

Tabla No.51 – Plan de acción establecido en la gestión de riesgos de Seguridad de la Información del proceso de Gestión de Información

8.2. Seguimiento del Riesgo

Para la vigencia 2026, el seguimiento de los Riesgos de Seguridad de la Información identificados por cada Proceso se llevará a cabo tres (3) veces al año. Esta actividad es fundamental para garantizar que las medidas de mitigación se realicen y que los riesgos sean gestionados adecuadamente en toda la Entidad.

El seguimiento se realiza en los siguientes periodos:

Periodo	Seguimiento
Enero a Abril	Mayo
Mayo a Agosto	Septiembre
Septiembre a Diciembre	Diciembre

Tabla No.52 - Seguimiento de los Riesgos de Seguridad de la Información

Estas revisiones periódicas permitirán ajustar las estrategias de seguridad de la información según sea necesario, asegurando así una protección continua y eficaz de los activos informativos de la organización.

Cada Proceso deberá reportar las evidencias de la aplicación y cumplimiento del Control y Plan definido por el líder del Proceso para la mitigación del riesgo en cada uno de los seguimientos que se realizaran en la vigencia.

¡Importante!

- En cada seguimiento se realizará un informe del cumplimiento de los Controles y Planes definidos.

- En los casos de materialización del riesgo, este deberá reportarlo de acuerdo con la "Metodología de administración de Riesgos" definida por la entidad.

Nota:
Para el desarrollo del Seguimiento del Riesgo, remitirse a la **"Metodología de Administración de Riesgos"** https://www.unidadvictimas.gov.co/NODE/45506.

8.2.1. Revisión y Actualización

La revisión y actualización de los mapas de riesgos se validan mínimo una (1) vez en cada vigencia en el marco de la metodología vigente y de manera oportuna ante cualquier modificación del proceso, estructura organizacional, objetivos estratégicos, modificación de controles derivados del seguimiento o de los eventos (materialización del riesgo).

Nota:
Para el desarrollo de la Revisión y Actualización, remitirse a la **"Metodología de Administración de Riesgos"** https://www.unidadvictimas.gov.co/NODE/45506.

8.2.2. Medición

Para la vigencia 2026, la medición del Tratamiento de los Riesgos de Seguridad de la Información en la **Unidad para las Víctimas** se llevará a cabo a través de un indicador específico. Este indicador permitirá evaluar y monitorear los riesgos reportados por los diferentes Procesos.

La periodicidad de los reportes asegurará una actualización constante del estado de los riesgos y la efectividad de las medidas implementadas. Cada reporte incluirá justificaciones detalladas y aporte de evidencias que respalden las acciones tomadas y los resultados obtenidos, proporcionando una base sólida para la toma de decisiones informadas y la mejora continua de la gestión de riesgos.

Para la implementación del Tratamiento de Riesgos de Seguridad de la Información vigencia 2026 se define el siguiente indicador.

Formula: $\frac{\text{Sumatoria de actividades ejecutadas que mitigaron riesgos}}{\text{Total de actividades programadas para mitigar riesgos}} * 50\% + \frac{\text{Sumatoria de controles con soportes de ejecución}}{\text{Total de controles identificados en la valoración de riesgos}} * 50\%$

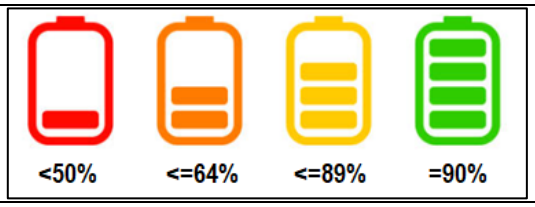	• Meta: 90% • Línea Base: 0% • Periodicidad: tres (3) al año. • Fuente: Plan Institucional. • Nivel: Nivel Nacional.

Imagen No. 2-Rangos de Tolerancia del Indicador.

La medición se realiza con un indicador que está orientado principalmente para el cumplimiento de los Controles y Planes definidos para mitigar los riesgos identificados de Seguridad de la Información.

8. Aprobación

ELABORÓ/ACTUALIZÓ	REVISÓ	APROBÓ
Nombre: Jerson Danilo Florez Parra **Cargo: Contratista**	Nombre: Joaquín Rojas Palomino **Cargo: funcionario**	Nombre: Alonso Rafael Ocampo Arrieta **Cargo: Jefe de la Oficina de Tecnologías de la Información** Comité Institucional de Gestión y Desempeño **Acta No:** **Fecha:**

Control de Cambios

Versión	Fecha	Descripción de la modificación
1	29/01/2026	Formulación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2026