Unidad para las Víctimas

COLOMBIA POTENCIA DE LA VIDA

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023-2026

UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS

Oficina de Tecnologías de la Información

www.unidadvictimas.gov.co

Síguenos en:

Línea de atención nacional: **01 8000 91 11 19**
Bogotá: **(601) 426 11 11**

Sede administrativa:
Carrera 85D No. 46A-65
Complejo Logístico San Cayetano
Bogotá, D.C.

Contenido

OBJETIVO

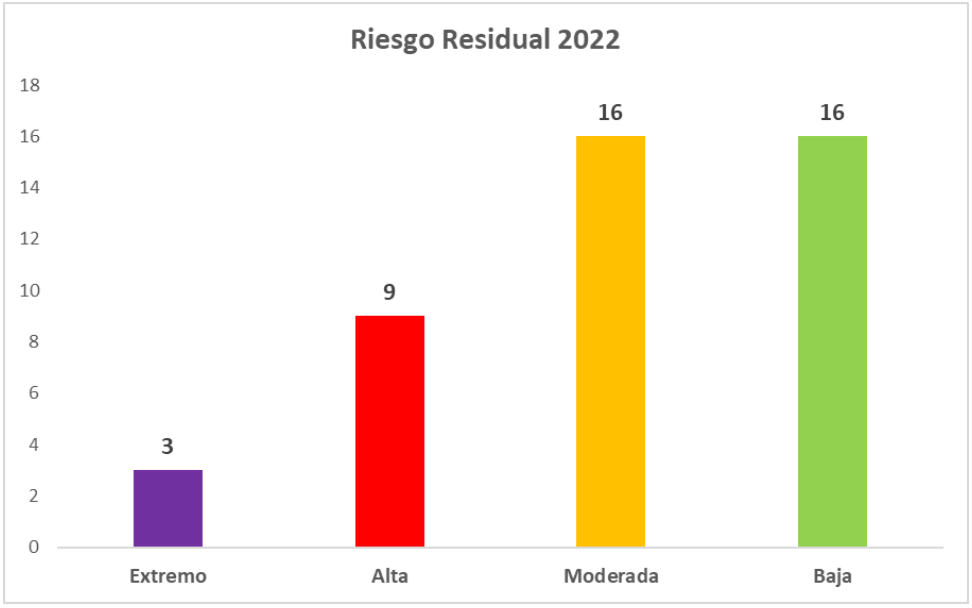
En el presente documento se presentan los planes de tratamiento al riesgo asociado al Sistema de Gestión de Seguridad y Privacidad de la Información para el correspondiente seguimiento y verificación al cumplimiento de los planes definidos en el marco de la metodología para la administración de riesgos establecida por la Unidad para la Atención y la Reparación Integral a las Víctimas.

ALCANCE

En el marco de los planes de tratamiento al riesgo se encuentran actualizados e identificados los riesgos de seguridad y privacidad de la información.

PLANES DE TRATAMIENTO AL RIESGO

Tomando como base el levantamiento de activos de información realizado en Julio del 2022 con el apoyo de los Enlaces del SIG de la Unidad para la Atención y Reparación Integral a las Víctimas, en la siguiente grafica se observa el nivel de riesgo residual con corte a octubre 2022[1]:



No Planes de tratamiento al riesgo: 39

[1] Riesgos de Seguridad y Privacidad de la Información 2022 actualizados.

Unidad para las Víctimas

Riesgos asociados al Sistema de Gestión de Seguridad y Privacidad de la Información:

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo Inherente	Descripción del control	Nivel de Severidad Riesgo Residual	Tratamiento	Plan de Acción
Realizar las actividades encaminadas al mejoramiento continuo del Sistema de Gestión de Seguridad de la Información en la Entidad. Actualización periódica de las partes interesadas de la entidad.	Posibilidad de pérdida económica y reputacional por no responder las necesidades y expectativas de las partes interesadas debido a no determinar las actividades encaminadas al mejoramiento continuo del sistema y a la falta de seguimiento en la actualización del contexto del SGSI.	Muy baja	Moderado	Alto	El proceso de control interno realiza auditorías anualmente de carácter interno al SGSI y /o Sistemas de información para determinar el cumplimiento de las políticas, lineamientos y normas de seguridad de la información. en caso de no presentar o realizar la auditoria el jefe de oficina solicita a control interno la auditoria , como evidencia se tiene el plan de auditoría (A 18.2.2 - A 18.2.3)	**Moderado**		Realizar la actualización de la caracterización del proceso de Gestión de la información para identificar las entreadas y salidas para el proceso de Gestión dela información (previo para actialización de las partes interesadas (ISO 27001:2013 - 4.2)
Adoptar el Modelo de Seguridad y Privacidad de la Información del MinTIC en la Entidad - requisito legal establecido por MIN TIC 00500 del 2021 para las entidades del estado	Posibilidad de pérdida reputacional por la indisponibilidad, divulgación o alteración no autorizada de información debido a la falta de seguimiento y actualización del modelo de madurez que debe mantener la entidad.	Muy baja	Mayor	Alto	El grupo de seguridad revisa anualmente o cuando ocurra cambios significativos la política del SGSI sea coherente con el modelo de Seguridad y Privacidad de la Información MSPI solicitado por MINTIC,en caso de no contar con actualización se aplicará la politica vigente, como evidencia se tiene el diligenciamiento del MSPI (A 5.1.2- A 18.2.2 - A 18.2.3)	**Alto**	Reducir - Mitigación	Realizar auditorías de carácter interno al SGSI y /o Sistemas de información para determinar el cumplimiento de las políticas, lineamientos y normas de seguridad de la información. (A 5.1.1, A 5.1.2, A 18.2.1, A 18.2.2 Y A 18.2.3)
Identificar y gestionar los activos que generan valor (manejo de la información) de la UARIV.	Posibilidad de pérdida económica y reputacional por la indisponibilidad, divulgación o alteración no autorizada de información debido a la desactualización del instrumento de Inventario de activos de información, mala clasificados de los activos de información de la entidad y a la calificación errada en la criticidad de los activos en cuanto a los pilares de seguridad.	Muy baja	Mayor	Alto	Los enlaces de cada proceso anualmente realizan la actualización del inventario de activos de información de la entidad, En caso de no realizar la actuaización el enlace del proceso reportará al jefe de oficina, como evidencia se cuenta con correo de aprobación e inventario de activos de cada proceso por parte de grupo de seguridad y privacidad de la información. (A 8.1.1 -A 8.1.2 -A 8.2.1)	**Alto**		Realizar los ajustes al Modelo Seguridad y Privacidad de la Información de acuerdo con las auditorias (A 5.1.1, A 5.1.2, A 18.2.1, A 18.2.2 Y A 18.2.3)
*Realizar análisis de vulnerabilidades y asociar los activos de información pertinentes. *Hacer investigación de incidentes de seguridad de la información, la divulgación de las lecciones aprendidas.	Posibilidad de pérdida reputacional por indisponibilidad, divulgación o alteración no autorizada de información debido al desconocimiento de los usuarios por aplicar adecuadamente el protocolo de incidentes y a la no ejecución de pruebas de vulnerabilidad o test de penetración.	Media	Mayor	Alto	El grupo de seguridad realiza semestralmente ejercicios de obtención de vulnerabilidades técnicas de los sistemas de información operados en la entidad, en caso de no realizar los ejercicios se reportará al jefe de oficina, como evidencia se tiene informe de vulnerabilidades técnicas a sistemas de información. (A 12.6.1 - A 12.6.2)	**Moderado**	Reducir - Mitigación	Se realiza la entrega de vulnerabilidades técnicas a cada uno de los lideres de los dominios involucrados para dar el correctivo, como evidencia se tiene el plan de remedición de vulnerabilidades. (A.12.6.1 Y A.12.6.2)
Promover, mantener y establecer la cultura en seguridad de la información en la Unidad para las Víctimas y partes interesadas con el propósito de generar un ambiente seguro frente al uso y cuidado de los activos de información.	Posibilidad de pérdida económica y reputacional por indisponibilidad, divulgación o alteración no autorizada de información debido a no comprender las debilidades, oportunidades, fortalezas y amenazas que puede presentar la UARIV respecto a la seguridad de la información por parte de los funcionarios, contratistas y operadores de la entidad.	Baja	Mayor	Alto	El grupo de seguridad define cada vez que presente incidentes, en el marco del procedimiento o protocolo "Gestión de Incidentes seguridad de la información", da tratamiento al evento de seguridad la cual mes cargado en la herramienta Aranda , en caso de no ser reportados seran reportados por el grupo de seguridad en la herramienta Aranda, Como evidencia se cuenta con el registro mensual en aranda. (A 16.1.2 - A 16.1.3 - A 16.1.4 - A 16.1.5 - A 16.1.6 - A 16.1.7)	**Alto**	Reducir - Mitigación	Realizar Capacitaciones a funcionarios, terceros y operadores para recibir educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo. (A. 7.2.2 A.16.1.6)

Gestión de la Información:

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo Inherente	Descripción del control	Nivel de Severidad Riesgo Residual	Tratamiento	Plan de Acción
Gestionar sistemas de información.(Sistema de Información/Aplicación en producción)	Posibilidad de pérdida económica y reputacional del proceso, del cliente interno (Unidad) y/o de las partes interesadas que este atiende por el Incumplimiento en la entrega y/o adquisición de desarrollo de sistemas de información, debido a: Falta de personal técnico o administrativo suficiente que cubra todos los roles para el desarrollo de software de acuerdo al ciclo de vida del desarrollo o los requerimientos adicionales; Desatención de los lineamientos del procedimiento formalizado por la OTI; El Cambio del recurso humano que se encuentra dentro del flujo desde la solicitud hasta la implantación del desarrollo de software impactan en el cumplimiento de entrega de los requerimientos y fechas establecidas; Requerimientos funcionales extensos que deben ser fragmentados según recursos del dominio para lograr entregar el producto por fases, presentando una brecha	Baja	Menor	Moderado	El personal del dominio de sistemas de información implementa y controla el ciclo de desarrollo a través de la herramienta de gestión de desarrollo según lo establecido en el procedimiento de sistemas de información y sus documentos de apoyo, bajo el cual se generan solicitudes de requerimientos por demanda bajo responsabilidad del área funcional, se realizan las asignaciones de actividades a los equipos de desarrollo presentes en la Unidad por etapa, roles y fechas según disponibilidad de los equipos de desarrollo, se reporte el avance, cierre de las actividades conforme a las fechas establecidas y se gestionan los impedimentos en caso de desviaciones (tales como reasignación de tareas o ampliación de tiempos de implementación), lo cual se evidencia en	**Bajo**	Aceptar	Recopilar la información técnica y funcional de los nuevos sistemas de información para garantizar el registro de derechos de autor, incentivar y fortalecer la construcción documental alrededor de los requerimientos y solicitudes con relación a sistemas de información y procesamiento de datos, como la misma gestión de cada uno de los colaboradores. (A.12.1.3)
Gestionar servicios e infraestructura TI. (Sistema de Información/Aplicación funcional; Sede dotada tecnológicamente; Validación de inventario de dotación tecnológica instalada y de planos de infraestructura tecnológica; Usuario con dotación tecnológica puntual instalada; Correo institucional creado, modificado o eliminado; Acceso remoto a servidores y bases de datos otorgado; Servicios de telefonía IP y/o funcionalidades especiales atendidos; Soporte tecnológico ejecutado)	Posibilidad de pérdida económica y reputacional del proceso, del cliente interno (Unidad) y/o de las partes interesadas que este atiende por la Indisponibilidad y/o inoportunidad de los servicios tecnológicos y/o de infraestructura TI para los procesos de la Unidad según los acuerdos de niveles de servicio establecidos por OTI, debido a: La falta de personal técnico y/o administrativo suficiente y/o idóneo para apoyar las tareas de soporte e infraestructura y servicios TI en la Unidad a nivel central y territorial al inicio de cada vigencia; Ingreso de personal (contratista o planta – concurso de méritos – contratación nueva administración) que retrase la atención de servicios y recursos tecnológicos durante la apropiación de su cargo; Falta de: 1) políticas y lineamientos establecidos para el manejo de la dotación tecnológica e infraestructura 2) de seguimiento y control a los lineamientos entre OTI,	Muy Alta	Moderado	Alto	El supervisor de los servicios e infraestructura tecnológica gestionados a través de proveedores TI, mensualmente realiza un seguimiento a cada uno de los acuerdos de niveles de servicio (ANS) establecidos en los contratos al cierre del periodo, con el fin de validar que el servicio recibido se encuentra dentro de los Acuerdos de Niveles de Servicios (ANS) establecidos; en caso de estar fuera de los rangos se aplican descuentos al valor facturado, lo que se evidencia en los informes de rendimiento generados y en la facturación (si aplica).	**Moderado**	Reducir - Mitigación	Dar continuidad a la ejecución de la estrategia "La OTI en territorio", conforme a los resultados del 2021 y la ejecución del 2022 en las direcciones territoriales y nivel central conforme a los recursos disponibles. (A.12.1.3)
Implementar los dominios de Uso y Apropiación e Información del marco de referencia de arquitectura TI vigente.	Posibilidad de pérdida reputacional del proceso, del cliente interno (Unidad) y/o de las partes interesadas que este atiende por el Incumplimiento en la implementación de los dominios de Uso y Apropiación e Información del marco de referencia de arquitectura TI vigente debido a: Ingreso de personal (contratista o planta, concurso de méritos) a la OTI que retrase la atención de servicios y recursos tecnológicos de los dominios durante la apropiación de su cargo; Ingreso de personal nuevo a la entidad que requiere aprendizaje en las herramientas IT; Debilidades en cuanto a la articulación con otros equipos de divulgación sobre	Baja	Menor	Moderado	El personal del dominio de Uso y Apropiación de TI formula y ejecuta un plan de uso y apropiación anual definiendo actividades por vigencia en función del resultado de indicadores y encuestas, herramientas y capacidades disponibles para fortalecer el uso y la apropiación de las tecnologías de la información, según las necesidades de los usuarios, la atención de lineamientos del marco de referencia de MinTIC en cuanto a este dominio, dejando como evidencia el plan aprobado y los soportes de ejecución de actividades allí	**Bajo**	Aceptar	Ejecutar proyectos u operaciones del dominio de información que contribuyan con la mejora de las capacidades de TI establecidas en el PETI, con el fin de optimizar el nivel de madurez TI definido para la vigencia. (A.12.1.3-A.12.1.1)

Gestionar la estrategia, el gobierno TI y la arquitectura empresarial. (Estrategia de TI, Actualización del PETI, Ejecución y medición desempeño del Portafolio de proyectos y operaciones TI, Proyecto TI estructurado, ejecutado y cerrado conforme al modelo definido)	Posibilidad de pérdida económica y reputacional del proceso, del cliente interno (Unidad) y/o de las partes interesadas que este atiende por la inadecuada gestión frente a la estrategia TI y/o la omisión de la alineación al Gobierno TI y a la arquitectura empresarial en la Unidad debido a: Limitación y/o disminución de la asignación de recursos presupuestales al proyecto de inversión de la OTI, afectando: prestación de los servicios tecnológicos y su renovación, promoción y/o continuidad de personal vinculado de prestación de servicios, proyectos de transformación digital, la implementación de las estrategias en el territorio, mejora de los sistemas de información, la implementación de la Arquitectura Empresarial, la implementación de las actividades de uso y apropiación sede nacional y territoriales; Reducción en el presupuesto asignado a la entidad y/o recortes presupuestales no contemplados durante la planeación de la vigencia por parte de Min Hacienda; Fluctuaciones en las condiciones del mercado que encarezcan el acceso al	Baja	Moderado	Moderado	El responsable de la gestión del portafolio de proyectos gestiona la definición de dicho portafolio de proyectos y/o las operaciones, conforme a las necesidades por demanda de la Unidad, asociándolos a uno de los dominios del marco de referencia de arquitectura TI Colombia, a los habilitadores, y/o a las capacidades TI del Plan Estratégico de Tecnologías de la Información (PETI) y realiza seguimiento a su ejecución en función del ciclo de vida de gestión de proyectos TI basado principalmente en el estándar PMBOK® del PMI®, avanzando en cuanto a la implementación de los lineamientos de MinTIC frente a los dominios, según la contribución que realice el proyecto u operación al dominio, capacidad o componente del PETI con el fin de lograr la transformación digital en alineación con la estrategia de la Unidad, del sector y del Plan Nacional de Desarrollo, conforme a lo establecido en el procedimiento de estrategia y gobierno TI	**Moderado**	Reducir - Mitigación	Realizar capacitaciones, talleres y/o socializaciones inscritos en el plan de uso y apropiación vigencia 2023: 1) Convocando a un funcionario de cada direccion territorial que apoye la resolución de problemas tecnológicos en el territorio frente a servicios y/o infraestructura TI. 2)A personal nuevo de TI de los diferentes dominios según material preparado por cada equipo de trabajo y 3) A los auditores en generalidades de servicios e infraestructura TI que les permita tener un sustento técnico y sin ambigüedades al momento de levantar no conformidades. (A.7.2.2)
Gestionar sistemas de información (Sistema de Información/Aplicación en producción) Gestionar servicios e infraestructura TI (Sistema de Información/Aplicación funcional; Acceso remoto a servidores y bases de datos otorgado)	Modificación o extracción de la Información alojada en los servidores o bases de datos asociada a las victimas, por parte de funcionarios o contratistas con acceso a la misma, para obtener un beneficio personal o para un tercero	Alta	Catastrófico	Extremo	El equipo de sistemas de información implementa el control de acceso a aplicativos mediante usuario y clave a los sistemas de información que gestionan información no publica. La frecuencia de implementación es por demanda según solicitudes de desarrollo y su evidencia es la funcionalidad implementada en el sistema de información. En caso de que no se implemente este control la aplicación no se lleva a producción.	**Alto**	Reducir - Mitigación	Actualizar el procedimiento de seguridad de la información, conforme a: 1) resultado de la auditoria ISO 27001 y seguimiento a no conformidades, 2)los lineamientos de MinTIC y del MIPG que apliquen, según disponibilidad de recursos y que sean susceptibles de ser implementados de acuerdo a la estrategia que se defina en la OTI para este fin. (A.12.1.1
* Dar trámite a las solicitudes de información realizadas por el cliente interno o entidades externas. * Alistar y disponer las fuentes y bases de datos de información de la población víctima de acuerdo con la necesidad, en las herramientas, aplicativos y visores utilizados por la SRNI	Posibilidad de pérdida reputacional por el uso indebido de la información dispuesta por la SRNI ocasionado por suplantación de usuarios para el acceso a las herramientas, debilidad de controles para el acceso a los datos.	Media	Catastrófico	Extremo	Cada vez que los procedimientos de la Subdirección Red Nacional de Información-SRNI reciban una solicitud de información a través de sus correos institucionales o plataforma aranda deben canalizarla y/o copiar lo emitido a los correos oficiales de la SRNI, así mismo, con el objetivo de tener la trazabilidad para los casos en que se dé respuesta mediante el correo individual institucional, se debe copiar al correo oficial los insumos entregados por parte de la SRNI. Como evidencia queda el envío a los correos oficiales con sus adjuntos (si los hubo) y socializaciones.	**Extremo**	Reducir - Mitigación	Indagar 2 veces en el año, en las mesas de trabajo desarrolladas con los articuladores territoriales, mediante video conferencias, subcomites, espacios formales, reuniones presenciales o correo electrónico, si se ha presentado uso indebido de las credenciales de acceso al portal de aplicaciones vivanto.

* Dar trámite a las solicitudes de información realizadas por el cliente interno o entidades externas. * Alistar y disponer las fuentes y bases de datos de información de la población víctima de acuerdo con la necesidad, en las herramientas, aplicativos y visores utilizados por la SRNI	Posibilidad de pérdida reputacional por indisponibilidad, divulgación o alteración no autorizada de información 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.	Media	Moderado	Moderado	El equipo SRNI realiza configuración de dispositivos con bloqueo por contraseña. Una contraseña para que el dispositivo salga del modo de suspensión en el que entra tras un período de inactividad. Medida que se complementa con el cifrado de la memoria y la clave solo está en poder de la SRNI. Se evidencia con las tablets utilizadas en los levantamientos de información. (A.6.1.2, A.9.2.1 Y A.9.2.3)	**Moderado**	Reducir - Mitigación	Socializar dos veces al año a los profesionales encargados semestralmente mediante correo y/o reunión sobre los lineamientos de seguridad establecidos por COMR (ISO27001:2013 -10.2)
Atención de Incidentes de Seguridad	Posibilidad de pérdida económica y reputacional por indisponibilidad, divulgación o alteración no autorizada de información provocado por Ciberdelincuencia que generan ataques a la entidad y debido al daño de los equipos de cómputo y red por la materialización de un incidente de seguridad.	Alta	Catastrófico	Extremo	El grupo de seguridad y privacidad de la información realiza revisión y seguimiento a las investigaciones automatizadas en defender ATP para la prevención y corrección de alertas de seguridad, esta actividad se realiza por demanda y como evidencia se cuenta con el registro de	**Moderado**	Reducir - Mitigación	Realizar una investigación de los incidentes más relevantes para la toma acciones de mejora correspondientes (A.16.1.6 y A.16.1.7)
Alinear las necesidades de negocio desde las diferentes disciplinas, evaluando proyectos que brindan propuestas de valor institucional a la entidad (Gestión de la Información - Arquitectura Empresarial)	Posibilidad de pérdida reputacional debido a la indisponibilidad o alteración de información por incumplimiento de políticas y lineamientos relacionados con integridad contempladas por los principios de arquitectura.	Muy Alta	Catastrófico	Extremo	El proceso de gestión de la información revisa anualmente las políticas y lineamientos del gobierno de la información para la Unidad como evidencia se tiene el documento publicado. En caso de no requerir actualización se comunicara por correo a las partes interesadas. Como evidencia se	**Extremo**	Reducir - Mitigación	El grupo de Gestión de información creará el Documento Marco de Referencia (A.12.1.1)
Servicio de soporte tecnológico y dotación tecnológica de equipos de cómputo y portátiles (Servicios TI)	Posibilidad de pérdida económica y reputacional por indisponibilidad, divulgación o alteración no autorizada de información debido a falla Técnica y /o humana en la atención del soporte, daño o hurto de equipos de cómputo asignados a los colaboradores de la Entidad.	Alta	Mayor	Alto	El 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, como evidencia se tiene la segregación de tareas en la herramienta Aranda. En caso de presentar problemas la herramienta aranda se tiene el consolidado de correo en soporteoti@unidadvictimas.com (A 6.1.1)	**Alto**	Reducir - Mitigación	Realizar Capacitaciones a funcionarios, terceros y operadores para recibir educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo. (A. 7.2.2 A.16.1.6)
Gestionar los servicios y capacidad tecnológica que soporta la operación n y las necesidades de la Unidad (Infraestructura)	Posibilidad de pérdida reputacional por indisponibilidad, divulgación o alteración no autorizada de información a causa a la no realización de las copias de respaldo por no implementar la política y/o protocolo para realizar backup de la información, una inadecuada gestión de identidades y control de acceso a los recursos y repositorios de información de la organización o causado por obsolescencia tecnológica en servidores	Alta	Mayor	Alto	El dominio de Infraestructura realiza ejecución diaria de Backup y redundancia de los mismos, como evidencia se tiene un informe del portal donde se observa la ejecución de BK y log de ejecución de BK de las bases de datos. En caso de generar error el backup este se lanza nuevamente. (A 12.3.1, A.17.2.1)	**Alto**	Reducir - Mitigación	El grupo de infraestructura procederá a realizar pruebas de restauración BK (A 12.3.1)
Gestionar los servicios y capacidad tecnológica que soporta la operación y las necesidades de la Unidad.(Sistemas de Información)	Posibilidad de pérdida reputacional por divulgación o alteración no autorizada de información debido a la ausencia de políticas y controles a nivel de dominio y sistemas de información.	Baja	Catastrófico	Extremo	Los líderes de los procesos solicitan por requerimiento la creación o inactivación de usuarios por la mesa de servicios de la Oficina de tecnologías de la información una vez se ingrese, retire o cambie de perfil un usuario (Funcionario, contratista o operador), como evidencia se tiene la	**Extremo**	Reducir - Mitigación	Implementar controles de inactivación de usuarios en los administradores de los diferentes sistemas de información (A.9.2.6)
Gestionar los servicios y capacidad tecnológica que soporta la operación y las necesidades de la Unidad. (Sistemas de Información)	Posibilidad de pérdida económica y reputacional por indisponibilidad, divulgación o alteración no autorizada de información provocado por la ausencia o falla en la ejecución del control de cambios o por nuevos desarrollos y/o actualizaciones del software a cargo del proceso de Gestión información.	Baja	Catastrófico	Extremo	El grupo de Sistemas de información aseguran las fuentes por Azure devops cada vez que sea aceptado y probado un cambio en los sistemas de información, en caso de nos ser aprobado el cambio este no se ejecutará, como evidencia se tiene repositorio en Azure Devops (A.17.2.1)	**Alto**	Reducir - Mitigación	Se diseña e implementa procedimiento formal de control de cambios el cual debe hacer cumplir para asegurar la integridad del sistema de información desde las primeras etapas de diseño hasta el mantenimiento del mismo. (A.12.1.2)

* Dar trámite a las solicitudes de información realizadas por el cliente interno o entidades externas. * Alistar y disponer las fuentes y bases de datos de información de la población víctima de acuerdo con la necesidad, en las herramientas, aplicativos y visores utilizados por la	Posibilidad de pérdida reputacional por indisponibilidad, divulgación o alteración no autorizada de información 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.	Media	Moderado	Moderado	El equipo SRNI realiza configuración de dispositivos con bloqueo por contraseña. Una contraseña para que el dispositivo salga del modo de suspensión en el que entra tras un período de inactividad. Medida que se complementa con el cifrado de la memoria y la clave solo está en poder de la SRNI. Se evidencia con las tablets utilizadas en los levantamientos de información. (A.6.1.2, A.9.2.1 Y A.9.2.3)	**Moderado**	Reducir - Mitigación	Realizar encriptación de la base de datos en el dispositivos (A.10.1.1 - A.10.1.2)
* Dar trámite a las solicitudes de información realizadas por el cliente interno o entidades externas. * Alistar y disponer las fuentes y bases de datos de información de la población víctima de acuerdo con la necesidad, en las herramientas, aplicativos y visores utilizados por la	Posibilidad de pérdida reputacional por acceso no autorizado a las herramientas de la SRNI (Correo,Sftp,Xroad, aranda y sherpoint, Modelo Integrado, BD, Portal de Aplicaciones Vivanto) debido a un acceso indebido a la Información de Identificación Personal, lo que traería como consecuencia usar la IIP con propósitos desconocidos o ilegales.	Muy Alta	Catastrófico	Extremo	Cada vez que se recepcione información, los líderes de los procedimientos de la SRNI del proceso de Gestión de la Información analizan el flujo de información de la SRNI para identificar si se debe limitar la recolección. En caso de no limitar la recoleccion se analizara el limitar el procesamiento de la IIP en las tareas realizadas por cada uno de ellos. Queda como evidencia el acta de reunión, los oficios, correos de solicitud y/o	**Extremo**	Reducir - Mitigación	Analizar el flujo de información en los procedimientos de SRNI para identificar si debe limitar la recolección y el procesamiento de la IIP en las tareas realizadas por cada uno de ellos. (A.13.2.1 - A.13.2.2)

Gestión Contractual:

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo Inherente	Descripción del control	Nivel de Severidad Riesgo Residual	Tratamiento	Plan de Acción
Elaborar las minutas de los contratos derivados de los procesos de contratación adelantados por la entidad, de acuerdo a la modalidad de contratación.	Posibilidad de pérdida reputacional por alteración no autorizada de la información de los contratos en el aplicativo SECOP II, debido al ingreso no autorizado y uso inapropiado de usuarios y contraseñas personales por parte de terceros.	Alta	Menor	Moderado	El profesional con perfil de uso en SECOP II genera alerta e informe de riesgo de suplantación o ingreso no autorizado a su usuario, cada vez que se evidencie un suceso sospechoso en la plataforma de SECOP II, a la coordinación del GGC y a SGSI con el objeto de establecer lo sucedido y dejar evidencia mediante correo electrónico toda vez que se presenten sucesos sospechosos. En caso de modificacion de la informacion del contrato en la plataforma SECOP II este se reportara a la travez de la mesa de servicios tecnologicos para que este sea escalado al SGSI. (A.12.6.1)	**Moderado**	Reducir - Mitigación	Reforzar la interiorización de los temas del SSI en el proceso contractual y Fortalecer el conocimiento en buen uso de herramientas tecnológicas (A.7.2.2)

Gestión Jurídica:

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo Inherente	Descripción del control	Nivel de Severidad Riesgo Residual	Tratamiento	Plan de Acción
Ejercer la defensa técnica judicial y extrajudicial de la Entidad y realizar el recaudo de las obligaciones y acreencias a favor de la Entidad y Saneamiento de bienes que se encuentran bajo la administración del FRV	Posibilidad de pérdida económica y reputacional ante las partes interesadas por la divulgación, alteración no autorizada o Indisponibilidad de la información registrada en documento digital debido a no contar con una de herramienta o aplicativo para almacenar la información del proceso y sus grupos de trabajo y la falta de disponibilidad de personal para solucionar requerimientos y desarrollos tecnológicos.	Muy Alta	Mayor	Alto	Los administrativos de respuesta judicial, de defensa judicial, gestión normativa y conceptos realizan copia de seguridad en OneDrive de las bases de datos utilizadas como herramienta de consulta y actualización de estado de los procesos o de información, con el objetivo de tener una copia actualizada de las bases de datos y evitar la pérdida de información general de los grupos de trabajo, esta copia se realiza directamente de las bases de datos actualizadas a diario. En caso de no realizarse el respaldo de la información cada coordinador debe remitir un correo de solicitud de esta actividad al administrativo. Queda de evidencia el respaldo de las bases de datos utilizadas por los grupos de trabajo de la Oficina Asesora Jurídica en la herramienta OneDrive dispuesta por la Unidad. (A.12.3.1)	**Alto**	Reducir - Mitigación	Realizar reunión semestral con la OTI para gestionar, revisar avances y realizar pruebas en el aplicativo tecnológico de la Entidad para la consulta y control de la información de los diferentes grupos de trabajo de la Oficina Asesora Jurídica. (A.14.2.8 - A.14.2.9)

Registro y Valoración

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo Inherente	Descripción del control	Nivel de Severidad Riesgo Residual	Tratamiento	Plan de Acción
Distribuir los formatos Únicos de Declaración -FUD- ó suministro de la herramienta de toma en línea a las oficinas del Ministerio Público para la recepción de la declaración junto a la documentación anexa.-Analizar, valorar y decidir sobre las solicitudes de la inclusión o no inclusión en el Registro Único de Víctimas.-Tramitar las solicitudes de novedades y/o actualizaciones.-Tramitar las diferentes órdenes judiciales allegadas a la Subdirección de Valoración y Registro (SVR).-Atender a las solicitudes de información, resolver los recursos y revocatorias interpuestos por las víctimas.-Tramitar las actuaciones administrativas correspondientes a presuntas víctimas que hayan ingresado al Registro Único de Victimas de manera fraudulenta.-Generar documentos robustos, boletines, notas y otros productos a demanda que aporten al conocimiento, analítica y memoria institucional, asociada a los diferentes procesos misionales de la Unidad para las Víctimas.	Posibilidad de pérdida reputacional ante las victimas 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.	Muy Alta	Catastrófico	Extremo	El líder del procedimiento reporta que realiza novedades o actualizaciones en el registro mensualmente informan sobre los requerimientos o solicitudes atendidas internamente al aplicativo ARANDA, esto con el fin de monitorear constantemente los incidentes presentados por parte del personal del operador y cuáles son las novedades o actualizaciones 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 el grupo de sistemas del operador. (A.16.1.2 - A.16.1.3 - A.18.2.2)	**Alto**	Reducir - Mitigación	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 en articulación con la oficina de tecnologías 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 (A.7.2.2)

Relación con el Ciudadano:

Proceso	Actividad	Redacción del riesgo	Probabilidad Inherent	Impacto Inheren	Nivel de Severidad Riesgo Inherente	Descripción del control	Nivel de Severidad Riesgo	Tratamiento	Plan de Acción
Relación con el ciudadano	Tramitar y elaborar la respuesta a peticiones quejas, reclamos y consultas interpuestos por los ciudadanos, víctimas, entidades y organismos de control.	Posibilidad de pérdida reputacional ante las victimas por incumplimiento de los protocolos de seguridad afectando la confidencialidad, integridad y/o disponibilidad de los sistemas de información y/o la información registrada en documento físico o digital, debido a el acceso no controlado a información sensible / confidencial, incidencias y caídas de los aplicativos o herramientas tecnológicas, desconocimiento de la política general y específica de Seguridad de la Información de la Unidad.	Muy Alta	Menor	Alto	El personal de apoyo del Grupo de Servicio al Ciudadano encargados de los canales de atención, suscriben el "Acuerdo De Confidencialidad De Usuarios De Herramientas Tecnológicas O Información De La Unidad Para La Atención Y Reparación Integral A Las Víctimas", cada vez que se solicitan usuarios de las herramientas. De lo contrario no se asignarán los usuarios. Con el objetivo de dar cumplimento a las políticas de seguridad de la información de la Unidad, es importante que los funcionarios y 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. En caso de que se venza el acuerdo, el usuario es deshabilitado. Como evidencias se cuenta con los acuerdos de confidencialidad suscritos por cada herramienta. (A.13.2.4)	**Moderado**	Reducir - Mitigación	El grupo de Seguridad y Privacidad de la Información sensibilizan a los usuarios del proceso en las pautas de seguridad para un adecuado manejo de los sistemas de información (A.7.2.2)

Gestión Interinstitucional:

Proceso	Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo Inherente	Descripción del control	Nivel de Severidad Riesgo	Tratamiento	Plan de Acción
Gestión Interinstitucional	Uso adecuado de los activos de información generados dentro de la Dirección de Gestión Interinstitucional	Posibilidad de pérdida reputacional ante nuestras partes interesadas por mal uso e Indisponibilidad de los activos de información críticos del proceso debido a falta de apropiación de las políticas y lineamientos de Seguridad de la Información.	Media	Menor	Moderado	El líder del Proceso de la Dirección de Gestión Interinstitucional y las Subdirecciones, semestralmente comunican a los colaboradores los lineamientos y protocolos de Sistema de Seguridad de la Información, en cumplimiento con los requisitos legales vigentes y la Norma Técnica Colombiana ISO-IEC 27001:2013, en caso de identificar incumplimientos o inconsistencias se reforzarán las socializaciones del tema, como evidencia se cuenta con correo de comunicación. (A.18.1.3)	**Moderado**	Reducir - Mitigación	El grupo de Seguridad y Privacidad de la Información realiza sensibilizaciones a los cuales a los usuarios del proceso asistirán para conocer las pautas de seguridad para un adecuado manejo de los sistemas de información (A.7.2.2)

Gestión Documental:

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo Inherente	Descripción del control	Nivel de Severidad Riesgo Residual	Tratamiento	Plan de Acción
Proporcionar el servicio de préstamos y consulta de expedientes, que se encuentren bajo la administración del Archivo de la Entidad.	Posibilidad de pérdida económica y reputacional por indisponibilidad y alteración no autorizada de los expedientes, por deterioro y no contar con las herramientas tecnológicas para evitar su materialización.	Baja	Moderado	Moderado	El grupo de Gestión Documental trimestralmente o dependiendo de la cantidad de correos que ingresen genera Backups de los PST de todos los correos que ingresan a la entidad , en caso de pérdida de información, se puede acceder a la búsqueda del físico, si son ingresados de manera presencial. Con el objetivo de salvaguardar la información que ingresa a la entidad. Observación: Se cuenta con informes diarios de radicación. Evidencia: Registro Fotográfico e informes diarios de radicación. (A.12.3.1)	**Moderado**	Reducir - Mitigación	Participar en las capacitaciones programadas por la OTI para contar con el conocimiento del en temas de seguridad de la Información y garantizar su cumplimiento en el proceso de Gestiòn Documental. (A.7.2.2)

Gestión para la Asistencia:

Actividad	Redacción del riesgo	Probabilidad Inherent	Impacto Inheren	Nivel de Severidad Riesgo Inherente	Descripción del control	Nivel de Severidad Riesgo	Tratamiento	Plan de Acción
Analizar, tramitar las solicitudes y realizar la colocación de recursos a los registros viables por concepto de Atención Humanitaria y Ayuda Humanitaria.	Posibilidad de pérdida reputacional por el incumplimiento ante las víctimas de los protocolos de seguridad, afectando la confidencialidad, integridad y/o la información registrada en documento físico o digital. Acceso no controlado a información sensible / confidencial, incidencias y caídas de los aplicativos o herramientas tecnológicas, desconocimiento de la política general y específica de Seguridad de la Información de la Unidad.	Media	Menor	Moderado	La Subdirección de Asistencia y Atención Humanitaria, a través de la línea de acción de administración y gestión de sistemas de información, suscriben el "Acuerdo De Confidencialidad De Usuarios De Herramientas Tecnológicas O Información De La Unidad Para La Atención Y Reparación Integral A Las Víctimas", cada vez que se solicitan usuarios de las herramientas. De lo contrario no se asignarán los usuarios. En caso de que se venza el acuerdo, el usuario es deshabilitado. Como evidencia se cuenta con los formatos de aceptación de acuerdos. (A.13.2.4)	**Bajo**	Aceptar	El grupo de Seguridad y Privacidad de la Información de la OTI sensibilizan a los usuarios del proceso en las pautas de seguridad para y un adecuado el manejo de los sistemas de información (A.7.2.2)

Gestión Financiera:

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo Inherente	Descripción del control	Nivel de Severidad Riesgo Residual	Tratamiento	Plan de Acción
Control y registro de información financiera en SIIF NACION II.	Posibilidad de pérdida económica y reputacional por divulgación y alteración no autorizada e indisponibilidad del aplicativo SIIF Nación, debido a acceso no permitido, falla, daño o degradación de equipos de computo.	Muy Alta	Moderado	Alto	La persona delegada como administrador del Aplicativo "Sistema Integral de Información Financiera -SIIF Nación; tramitar a solicitud de la coordinación del Grupo de Gestión Financiera y Contable, la asignación de usuario que le permita el acceso a la información a través de un usuario asignado por Min hacienda. En caso de no recibir respueta del tramite de la solicitud nuevamente se re-envia solicitud. Como evidencia se cuenta con el formato diligenciado y los soportes requeridos, y autorización de acceso a la herramientas, o correos de solicitud de usuario, de acuerdo a las necesidades de la operación. (A.9.2 - A.9.2.1 - A.9.2.2)	**Moderado**	Reducir - Mitigación	Correos de incidencias y solicitudes de apoyo a la mesa de ayuda de Min hacienda. (A.16.1.2 - A.16.1.5)
Control y registro de información financiera en SIIF NACION II. Mediante Firma Digital.	Posibilidad de pérdida económica y reputacional por acceso no autorizado a tokens o firmas digitales, como consecuencia de captura de credenciales transferidas durante el ingreso vía web, debido a acceso no permitido, espionaje o ingeniería social, o suplantación de usuarios, robo de token o dispositivos autorizados.	Media	Moderado	Moderado	La persona delegada de administrar las firmas certificadas, mensualmente debe actualizar y reportar a la Coordinación del Grupo de Gestión Financiera y Contable, y a los usuarios autenticados las actualizaciones y fechas de vencimiento del dispositivo o token asignado, cuando la operación lo requiera. En el caso de los usuarios con asignación de token, la Firma Certificadora alerta por medio de correo electrónico informando el vencimiento de la firma digital con quince días de antelación. Como evidencia queda el correo y el informe actualizado. (A.9.1.2 - A.9.2 - A.9.2.1 - A.9.2.3 - A.9.2.5)	**Moderado**	Reducir - Mitigación	Reportar Firma Certificadora y Coordinación GGFC, Correos de incidencias y solicitudes de apoyo a la firma certificadora o proveedor de los dispositivos para firmas digitales. (A.9.1.2 - A.9.2 - A.9.2.1 - A.9.2.3 - A.9.2.5)

Comunicación Estratégica:

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo Inherente	Descripción del control	Nivel de Severidad Riesgo Residual	Tratamiento	Plan de Acción
Difundir la gestión institucional y la ley a través de los diferentes medios de comunicación tanto internos como externos	Posibilidad de pérdida económica y reputacional ante nuestras partes interesadas, por quejas o sanciones ocasionados por la generación de comunicación externa y/o interna inadecuada debido a ataques cibernéticos como los que han tenido otras páginas web del estado, al desconocimiento de los lineamientos de seguridad de la información por parte de los usuarios y a que no existe comunicación sobre alertas que afecten la información o que las políticas de los prestadores de conexión a redes sociales modifican las funcionalidades en sus plataformas.	Muy baja	Mayor	Alto	El grupo de comunicación digital de la Oficina Asesora de Comunicaciones, tiene establecido un código de verificación en dos pasos que se activa cada vez que alguno de los funcionarios autorizados con contraseña acceden desde otro dispositivo a cualquiera de las redes sociales de la Unidad. Los códigos solo serán recibidos por el funcionario de planta que hace parte del equipo digital. Si durante el desarrollo de la labor diaria alguna contraseña debe ser delegada a alguna persona diferente a los autorizados, será cambiada inmediatamente terminada la labor. Dichas modificaciones y los recibos de los códigos serán reportadas por parte de alguno de los integrantes del grupo digital. (A.9.4.2 - A.10.1.1 - A.10.1.2)	**Moderado**	Reducir - Mitigación	A partir de las socializaciones recibidas en privacidad y seguridad de la información se seguiran todas las recomendaciones y se pondrán en práctica los lineamientos al respecto (A.7.2.2)

Direccionamiento Estratégico

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo Inherente	Descripción del control	Nivel de Severidad Riesgo Residual	Tratamiento	Plan de Acción
Implementar las estrategias establecidas por el Sistema de Seguridad de la Información al interior del proceso	Posibilidad de pérdida reputacional ante los funcionarios por la divulgación o alteración no autorizada de los activos de información (Recurso Humano), debido a ausencia o insuficiencia de copias de respaldo, falta de apropiación de las políticas de privacidad de la información y protección contra virus y/o código malicioso, ausencia o insuficiencia de documentación de uso y/o administración.	Baja	Moderado	Moderado	El profesional de la OAP, se encarga de revisar e inactivar los usuarios, cuando se retiran de la Unidad, o cambian de proceso en la herramienta SISGESTION, módulos Plan de Acción y SIG. Esta actualización se realiza mediante correo electrónico. En caso de que no se solicite una revisión, la misma se realizara de manera trimestral para mantener la plataforma actualizada. Como evidencia quedan correos electrónicos. (A.9 - A.9.1.1 - A.9.2)	**Moderado**	Reducir - Mitigación	Diseño de estrategia lúdico - pedagógica para apropiación de los Sistemas de Gestión. (A.7.2.2)

Participación y Visibilización

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo Inherente	Descripción del control	Nivel de Severidad Riesgo Residual	Tratamiento	Plan de Acción
Actividades propias del proceso	Posibilidad de pérdida económica y reputacional ante las partes interesadas y sanciones por entes de control por divulgación o alteración no autorizada e indisponibilidad de los Activos de tipo Talento Humano del proceso, debido a la ausencia o insuficiencia de procedimientos de Monitoreo y de controles para la protección de la información en el almacenamiento, al acceso no controlado a información sensible / confidencial, falta de conectividad o fallas tecnológicas.	Baja	Moderado	Moderado	Los enlaces SIG del proceso, se articulan con la OTI, para hacer la migración a One Drive de toda la información del proceso (Está migración será desarrolla por demanda), con el fin de tener la información organizada, además de esto generar un mayor control sobre la misma, con lo cual se minimizaría la materialización del riesgo. En caso de que esa articulación no sea efectiva se enviará correo a la OTI y al responsable de la información con el fin de realizar dicha migración. Como evidencia quedan los correos electrónicos. (A.12.3 - A.12.3.1)	**Moderado**	Reducir - Mitigación	Solicitar a la OTI la socialización de los temas y procedimientos asociados al Sistema. (A.7.2.2)

Unidad para las Víctimas

Reparación Integral

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo Inherente	Descripción del control	Nivel de Severidad Riesgo	Tratamiento	Plan de Acción
Transversal al Proceso Reparación Integral.	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.	Baja	Mayor	Alto	Los administradores de las herramientas tecnológicas del Proceso Reparación Integral, suscriben el "Acuerdo de confidencialidad de usuarios de herramientas tecnológicas o información de la unidad para la atención y reparación integral a las víctimas", cada vez que se solicitan usuarios de las herramientas (Unidad, proveedores externos (operadores) y otros. De lo contrario no se asignarán los usuarios. En caso que se venza el acuerdo, el usuario es deshabilitado. Como evidencias se cuenta con los acuerdos de confidencialidad suscritos por cada herramienta y la inhabilitación de usuarios. (A 13.2.4).	**Moderado**	Reducir - Mitigación	Sensibilizar a los colaboradores para que hagan uso responsable en el acceso y manejo de la información de la Dirección de Reparación. (A 7.2.2)

Unidad para las Víctimas

Gestión Administrativa

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo Inherente	Descripción del control	Nivel de Severidad Riesgo Residual	Tratamiento	Plan de Acción
Controlar y hacer seguimiento a la atención de los servicios generales necesarios para el buen funcionamiento de la entidad (papelería, vigilancia, seguros, transporte, aseo y cafetería, mantenimiento)	Posibilidad de pérdida económica y reputacional por indisponibilidad de activos de información debido a la falta de controles de acceso físico y perimetrales a edificaciones y recintos de la entidad ante el ingreso de personal no autorizado.	Baja	Menor	Bajo	El proceso de Gestión Administrativa realiza la contratación de seguridad y vigilancia, asignando personal idoneo y camaras de seguridad , con el objetivo de garantizar la seguridad y custodia de los bienes de la entidad. (A.11.1.2) Evidencia; Contrato de servicio de Vigilancia en las sedes de la entidad	**Bajo**	Aceptar	Revisar los lineamientos establecidos en el contrato de vigilancia y solicitar las minutas , audifonos auriculares y manos libres para radio con el objetivo incrementar la comunicación y seguridad en la sede donde funcione la entidad. (A.15.2.1)
Todos los procedimientos soportados en la sede Nivel Central. Riesgo Seguridad de la Información	Posibilidad de pérdida reputacional ante los colaboradores de la Entidad por indisponibilidad de activos fijos y documentación, debido a perdida y/o daño de información como consecuencia de la falla en los equipos por cortes de energía e interrupción en la planta eléctrica.	Muy baja	Menor	Bajo	El grupo de gestión Administrativa realiza seguimiento a la administración del complejo, el cual realiza pruebas y mantenimiento periódico a la planta de manera bimensual con el objetivo de garantizar la continuidad del servicio y tomar medidas correctivas.Evidencia: Correo electronico administración de la sede la entidad (A.11.2 - A.11.2.2 - A.11.2.4)	**Bajo**	Aceptar	Solicitar a la Administración la revisión y solución del funcionamiento de las UPS. (A.11.2.2 - A.11.2.4)

Control Interno Disciplinario

Adelantar las actuaciones Disciplinarias y Administrativas, contra los servidores y exservidores públicos de la entidad, originadas en la incursión de faltas disciplinarias.	Posibilidad de pérdida reputacional ante las partes interesadas, por la pérdida de la reserva legal debido a una indebida custodia de los documentos físicos y tecnológicos que reposan en el plenario de las actuaciones disciplinarias que están a cargo del Grupo Control Interno Disciplinario.	Baja	Menor	Moderado	Los colaboradores del proceso asisten a las capacitaciónes y socializaciones brindadas por la OTI cada vez que se programen con el fin de dar cumplimiento a la implementacion de la política del Sistema de Gestion de seguridad y privacidad de información, prevención y apropiación de conocimientos del Sistema. En caso de no asistir se comparte la citación de la siguiente capacitacion y/o socialización.Como evidencia se cuenta con la lista de asistencia, acta de la socialización y grabación de la misma (A.7.2.2)	**Moderado**	Reducir - Mitigación	Por parte del Coordinador del Grupo de Control Interno Disciplinario se solicitará una reunión para que desde la Oficina de Tecnologias 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. Como evidencia quedará Acta de Reunion y compromisos. (A.12.3.1) (A.9.2.2 - A.9.2.3)

Prevención Urgente y Atención en la Inmediatez

Ejecutar los controles que se generen como resultado del análisis, evaluación y calificación de los aspectos e impactos ambientales, los peligros que afecten la seguridad y la salud en el trabajo, los activos de seguridad de la información y los riesgos operativos y de corrupción	Posibilidad de pérdida económica y reputacional ante las partes interesadas y sanciones por entes de control por divulgación o alteración no autorizada, indisponibilidad de los activos asociados a información y/o talento humano debido a la ausencia o insuficiencia de procedimientos de Monitoreo y controles para la protección de la información en el almacenamiento o el acceso no controlado a información sensible / confidencial.	Muy baja	Mayor	Alto	Los funcionarios, contratistas y colaboradores de la Subdirección de Prevención y Atención de Emergencias deben realizar Trimestralmente una copia del respaldo de la información en la carpeta SharePoint destinada para salvaguardar la información del proceso, con el fin de resguardar la información. En caso de registrarse la no realización del respaldo de la información por parte de algún colaborador, se enviará un correo electrónico impulsando la importancia de la realización del almacenamiento de la información en las herramientas dispuestas para tal fin. (A.12.3 - A.12.3.1)	**Alto**	Reducir - Mitigación	Los colaboradores del proceso asistirán a las capacitaciónes y socializaciones brindadas por la OTI cada vez que se programen con el fin de dar cumplimiento a la implementacion de la política del Sistema de Gestion de seguridad y privacidad de información, prevención y apropiación de conocimientos del Sistema. (A.7.2.2)

Gestión de Talento Humano

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Nivel de Severidad Riesgo Inherente	Descripción del control	Nivel de Severidad Riesgo Residual	Tratamiento	Plan de Acción
Administrar historias laborales y el Sistema Tecnológico KACTUS. Implementar, con el acompañamiento del GGAD, las TRD mediante la elaboración de los inventarios documentales de los archivos de gestión del total de las series y subseries de la TRD de la dependencia. Clasificar, con el acompañamiento del GGAD la documentación electrónica o digital bajo la estructura de las TRD (series y subseries) en las herramientas tecnológicas disponibles para tal fin. Participar en las jornadas del plan de capacitación del sistema de gestión documental.	Posibilidad de pérdida económica y reputacional ante los funcionarios de la Unidad y Órganos de Control por la alteración o divulgación no autorizada de la información asociada a historias laborales, al sistema KACTUS y al manejo debido al uso inapropiado del sistema, como también al uso inapropiado de los formatos y tablas de retención documental de la información física y la alta rotación de personal e incumplimiento de los lineamientos de Seguridad de la información.	Media	Moderado	Moderado	El profesional valida en el sistema tecnológico KACTUS los roles autorizados y genera las alertas conforme a las novedades de ingreso, traslados y retiro del personal, cada vez que se evidencie un cambio de roles en el sistema, procederá con la actualización del sistema. Evidencia: Correo electrónicos y log de auditoría de la herramienta tecnológica. (A.7.1.1 - A.7.1.2 - A.7.3.1 - A.9.2.1)	**Moderado**	Reducir - Mitigación	Implementar controles de inactivación de usuarios con los administradores del sistema tecnológico KACTUS. Evidencia Correo Electrónico. (A.9.2.1)
					El 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, Hoja De Control Archivos De Gestión y Formato De Préstamo De Documentos Y/O Expedientes. (A.7.1.1-A.7.1.2-A.7.3.1-A.8.1.1-A.8.1.2-A.8.1.4 - A.8.3.1-A.12.1.1)			Realizar una reinducción y socialización al personal responsable de la gestión y disposición de la información de las historias laborales. Evidencia listado asistencia capacitación. (A.7.2.2)

Unidad para las Víctimas

CONTROL DE CAMBIOS

ELABORÓ	REVISÓ	APROBÓ
Nombre: Johanna Polanía Martinez **Cargo: Contratista**	Nombre: Darío Eduardo Muñetón Zuluaga **Cargo: Jefe de la Oficina de Tecnologías de la Información** Nombre: Joaquín Rojas Palomino **Cargo: Contratista**	Comité Institucional de Gestión y Desempeño **Acta No:** **Fecha:**