



El futuro  
es de todos

Unidad para la atención  
y reparación integral  
a las víctimas

2022

# Plan de Tratamiento de Riesgos de Seguridad de la Información 2022

*Unidad para la Atención y Reparación a las  
Víctimas*

*Oficina de Tecnologías de la Información - OTI*



SC-CER512366



SC-CER814217



## Contenido

OBJETIVO.....	2
ALCANCE.....	2
PLANES DE TRATAMIENTO AL RIESGO .....	2
Riesgos asociados al Sistema de Gestión de Seguridad de la Información .....	3
Gestión de la Información .....	5
Gestión Administrativa:.....	8
Gestión Jurídica: .....	9
Reparación Integral .....	10
Gestión De Talento Humano .....	11
Gestión Financiera.....	12
CONTROL DE CAMBIOS .....	13

## OBJETIVO

En el presente documento se consolidan los planes de tratamiento de los riesgos asociados al Sistema de Gestión de Seguridad de la Información, para el correspondiente seguimiento y verificación, en el marco de la metodología para la administración de riesgos establecida por la Unidad para la Atención y Reparación Integral a las Víctimas.

## ALCANCE

El actual plan de tratamiento se realiza con base a los riesgos de Seguridad Información/Digital identificados en el mapa de riesgos institucionales de la Entidad. Los cuales se encuentran publicados en la página web de la entidad <https://www.unidadvictimas.gov.co/es/mapa-de-riesgos-institucional-corrupcion-y-gestion/60377>.

## PLANES DE TRATAMIENTO AL RIESGO

La gestión de riesgos permite identificar específicamente el activo de información que será afectado y los controles establecidos para mitigar su riesgo inherente y determinar el nivel de riesgo residual, cuyo nivel establece si se requiere diseñar el respectivo plan de tratamiento. A continuación, se relacionan la cantidad de riesgos categorizados por el nivel de riesgo residual:



No Planes de tratamiento al riesgo :24



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

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Riesgo Inherente	Descripción del control	Riesgo Residual	Tratamiento	Plan de Acción
Adoptar el Modelo de Seguridad y Privacidad de la Información del MinTIC en la Entidad - requisito legal establecido por MIN TIC Res 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 para que sea coherente con el modelo de Seguridad y Privacidad de la Información MSPÍ del MINTIC, como evidencia se tiene el diligenciamiento del MSPÍ (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)
					El grupo de Seguridad diligencia anualmente el reporte de madurez del MSPÍ. (A 5.1.1 - A 5.1.2 - A 18.2.2 - A 18.2.3)			Realizar los ajustes al diligenciamiento del instrumento del Modelo Seguridad y Privacidad de la Información de acuerdo con las auditorías (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, 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 líderes de los dominios involucrados para dar el correctivo, como evidencia se tiene el plan de remediación de vulnerabilidades. (A.12.6.1 Y A.12.6.2)
					El grupo de seguridad define cada vez que presente cambios significativos de políticas específicas de seguridad de la información las reglas de instalación de software por parte de los usuarios, como evidencia se tiene la resolución de políticas de seguridad de la Información (A. 12.5.1, A.12.6.2)			Se realiza el seguimiento al tratamiento y remediación de las vulnerabilidades halladas en la entidad, como evidencia se tiene el informe de cierre de vulnerabilidades (A.12.6.1)
					El grupo de seguridad documenta y realiza la atención de los incidentes y eventos en el marco del procedimiento o protocolo de "Gestión de Incidentes seguridad de la información", los cuales se cargan en la herramienta 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)			Realizar una investigación de los incidentes más relevantes para la toma acciones de mejora correspondientes (A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6 y A.16.1.7)
					Diariamente el grupo de infraestructura gestiona con el centro de datos la generación de copias de respaldo de servidores de aplicación, base de datos y file servers con una frecuencia diaria y/o mensual según la criticidad de la información. Como evidencia se tienen registros donde se realiza la confirmación de backups. (A 12.3.1)			Realizar un repositorio de lecciones aprendidas para resolver incidentes de seguridad y reducir la posibilidad de impacto en incidentes futuros (A.16.1.6)



Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Riesgo Inherente	Descripción del control	Riesgo Residual	Tratamiento	Plan de Acción
"Promover, mantener y establecer la cultura de seguridad de la información en la Unidad para las Víctimas y partes interesadas."	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 documenta y realiza la atención de los incidentes y eventos en el marco del procedimiento o protocolo de "Gestión de Incidentes seguridad de la información", los cuales se cargan en la herramienta 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)	Moderado	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)
					El grupo de seguridad define cada vez que presente cambios significativos la política para la gestión de activos y/o el Instructivo para la Construcción y Mantenimiento del Inventario de Activos de Información, como evidencia se tiene la política y procedimiento vigente. (A 5.1.1, A 5.1.12 A 8.1.3)			
					El grupo de seguridad establece cada vez que se llegue al vencimiento el plan de capacitación, sensibilización y comunicación de seguridad y privacidad de la información, como evidencia se tiene el documento Plan de capacitación sensibilización y comunicación de seguridad y privacidad de la información vigente. (A 7.2.2)			
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 servicios TI realiza la actualización del sistema Operativo Windows 7 a Windows 10 en los equipos de cómputo de la entidad de manera permanente, como evidencia se tiene el registro de membrecías Windows 10 en la herramienta Defender ATP. (A. 11.2.4)	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)
El grupo de seguridad y privacidad de la información realiza revisión y seguimiento a las investigaciones automatizadas en la herramienta 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 investigaciones automatizadas en la herramienta defender ATP. (A 12.2.1)								



Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Riesgo Inherente	Descripción del control	Riesgo Residual	Tratamiento	Plan de Acción
					<p>El grupo de seguridad y privacidad gestiona el envío periódico de flash informativos y realiza ejercicios de toma de conciencia a los usuarios para proteger la información contra código malicioso, como evidencia se tiene el envío de flash informativos y lista de asistencia de las sesiones realizadas para la toma de conciencia en temas relativos a seguridad de la información. (A 16.1.6)</p> <p>El grupo de seguridad documenta y realiza la atención de los incidentes y eventos en el marco del procedimiento o protocolo de "Gestión de Incidentes seguridad de la información", los cuales se cargan en la herramienta 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)</p>			Realizar un repositorio de lecciones aprendidas para resolver incidentes de seguridad y reducir la posibilidad de impacto en incidentes futuros. (A.16.1.6 y A.16.1.7)

*Gestión de la Información:*

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Riesgo Inherente	Descripción del control	Riesgo Residual	Tratamiento	Plan de Acción
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	<p>El proceso de gestión de la información define y construye las políticas y lineamientos del gobierno de la información para la Unidad 2021, el cual será entregado el día 30 de noviembre 2021, como evidencia se tiene el documento. (A 5.1.1 - A 5.1.2 - A 6.1.1)</p> <p>El grupo de infraestructura realiza periódicamente el control de Acceso a Bases y bodegas de datos en el marco del procedimiento de dominio Infraestructura TI una vez esta sea creada, como evidencia se tiene el correo de implementación del control por parte de infraestructura (A.9)</p> <p>El grupo de infraestructura gestiona con el centro de datos la generación de copias de respaldo de servidores de aplicación, base de datos y file servers con una frecuencia diaria y/o mensual según la criticidad de la información, con el fin de disponer de una copia de la información que pueda ser recuperada si se requiere. En caso de que no se efectuó la copia conforme a lo establecido, se procede a diagnosticar de manera inmediata la causa, tomar acciones y a realizar nueva copia. Como evidencia se tienen registros</p>	Extremo	Reducir - Mitigación	<p>El grupo de Gestión de información creará el Documento Marco de Referencia (A.12.1.1)</p> <p>Ejecutar pruebas periódicas de restauración de copias de seguridad (A 12.3.1)</p>



Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Riesgo Inherente	Descripción del control	Riesgo Residual	Tratamiento	Plan de Acción
					donde se realiza la confirmación de Backus. (A 12.3.1)			
"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	<p>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. (A 12.3.1, A.17.2.1)</p> <p>El grupo de Infraestructura revisa anualmente o cuando ocurran cambios significativos el procedimiento de acceso a servidores, como evidencia se tiene el procedimiento vigente. (A 12.1.1)</p> <p>Diariamente el grupo de infraestructura gestiona con el centro de datos la generación de copias de respaldo de servidores de aplicación, base de datos y file servers con una frecuencia diaria y/o mensual según la criticidad de la información. Como evidencia se tienen registros donde se realiza la confirmación de backups. (A 12.3.1)</p>	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 n y las necesidades de la Unidad (Infraestructura)	Posibilidad de pérdida reputacional debido a la indisponibilidad de información por daño de los equipos de comunicaciones	Alta	catastrófico	Moderado	<p>El grupo de infraestructura cuenta con disponibilidad de equipos de red para realizar cambios cuando estos presenten daños del equipo afectado, los equipos se cuentan en modalidad de arriendo como evidencia se cuenta correo de solicitud de cambio al proveedor (A.17.2.1 - A 13.1.1)</p> <p>El grupo de infraestructura realiza copias de seguridad de los equipos de red cada vez que presente cambio de configuración en estos, como evidencia se cuenta con repositorio de las copias de seguridad (a.17.2.1 - A 13.1.1)</p>	Bajo	Reducir - Mitigación	Se cuenta con un esquema de modalidad de servicio de arrendamiento de los equipos de red, el cual es remplazado en caso de daño )
Gestionar los servicios y capacidad tecnológica que soporta la operación y las necesidades de la Unidad	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	<p>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 u operador), como evidencia se tiene la solicitud en la herramienta defender ATP. (A 9.2.1 - A.9.2.2 - A 9.2.3)</p> <p>Infraestructura una vez reciba la solicitud de inactivación de buzones de correo será replicada a los administradores de los sistemas de</p>	Extremo	Reducir - Mitigación	Implementar controles de inactivación de usuarios en los administradores de los diferentes sistemas de información (A.9.1.1 - A.9.2.2 -A.9.2.3)



Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Riesgo Inherente	Descripción del control	Riesgo Residual	Tratamiento	Plan de Acción
(Sistemas de Información)					<p>información por medio de correo electrónico, como evidencia se tiene el correo enviado a los administradores del sistema. (A 9.2.1)</p> <p>El dominio de Servicios TI valida que las máquinas se encuentren en el dominio de la Unidad una vez sea entregada en operación el equipo al usuario (funcionario, contratista o operador), como evidencia se tiene el registro del equipo en el dominio (a.13.1.2 A.13.1.3)</p> <p>El dominio de infraestructura realiza una configuración estándar de usuario (no administrador) a todas las cuentas que entregan al usuario final, en caso de necesitar un perfil administrador el usuario realiza solicitud Aprobación Permiso Admin al grupo de seguridad, como evidencia se tiene el correo de aprobación o negación del requerimiento de la solicitud según criterios de aprobación. (A.9.2.2 - A.9.4.2)</p> <p>Cada vez que se realice cambio en la política de contraseñas el Grupo de Seguridad solicita al dominio de infraestructura aplicar política y complejidad de contraseñas desde el directorio activo, como evidencia se tiene el correo de respuesta por parte del grupo de infraestructura (A.9.4.3)</p>			
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	<p>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, como evidencia se tiene repositorio en Azure Devops (A.17.2.1)</p> <p>El grupo de Sistemas de información aseguran la documentación sobre los códigos fuentes una vez modificados, como evidencia se tiene repositorio de fuentes en Devops (A 9.4.5 - A 14.2.1)</p> <p>El grupo de Sistemas de información asigna roles específicos para el acceso a repositorios los cuales son parametrizados en los sistemas de información, como evidencia se tiene repositorio en los sistemas de información (A 9.2.3 - A 9.2.2)</p> <p>El dominio de Sistemas de información aplica anualmente la lista de chequeo de Seguridad de la información a cada uno de los sistemas de información a cargo, como evidencia se tiene la lista de chequeo de Seguridad de la información (A.14.2.8)</p>	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.14.2.2 - A.12.1.2)





Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Riesgo Inherente	Descripción del control	Riesgo Residual	Tratamiento	Plan de Acción
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 debido a la ausencia en la validación de los criterios de aceptación en el software a nuevas funcionalidades y/o actualizaciones del Sistemas de Información.	Baja	Menor	Moderado	El dominio de Sistemas de información ejecuta el Procedimiento desarrollo sistemas de información en cada uno de los requerimientos realizados, Como de evidencia se tiene la lista de verificación de Seguridad de la Información del Sistema de Información (A.14.2.2) El dominio de Sistemas de información atiende cada uno de los requerimientos de acuerdo con el Formato De Especificación De Requerimientos De Software V1 y Formato de Implementación de Software V2 diligenciado por el proceso solicitante, como evidencia se tiene los formatos diligenciados para cada uno de los desarrollo o modificaciones a los Sistemas de información (a.14.2.5)	Bajo	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.14.2.2 - A.12.1.2)

*Gestión Administrativa:*

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Riesgo Inherente	Descripción del control	Riesgo Residual	Tratamiento	Plan de Acción
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 San Cayetano, 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. (A.11.2 - A.11.2.2 - A.11.2.4) El grupo de Gestión Administrativa realiza seguimiento a la administración del complejo San Cayetano, el cual realiza pruebas y mantenimiento anual a las UPS con el objetivo de garantizar la continuidad del servicio. (A.11.2 - 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)



Gestión Jurídica:

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Riesgo Inherente	Descripción del control	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)



### Reparación Integral

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Riesgo Inherente	Descripción del control	Riesgo Residual	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.	Bajo	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 de 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.8.1.3 - A.8.2.3)
					Los Administradores de los Sistemas de información del proceso Reparación Integral, permanentemente cuentan con formularios de inicio de sesión que sólo permiten el acceso a la información de la Dirección de Reparación (de acuerdo a los perfiles asignados) a través de un usuario de autenticación como de una contraseña segura, de lo contrario no se tendrá acceso a las mismas. Este usuario se asigna mediante la suscripción de un acuerdo de confidencialidad. Como evidencia se cuenta con la relación mensual de usuarios de las herramientas y los acuerdos de confidencialidad suscritos. ( A 9.2.3 - A 9.2.4 - A 9.4.1 - A 9.4.3 )			Implementar nuevas acciones de seguridad para el uso de los sistemas de información de la Dirección de Reparación en articulación de la Oficina de Tecnologías de Información. (A.14.1.1 - A.14.1.2 - A.14.1.3 - A.14.2.1 - A.14.2.2 - A.14.2.3 - A.14.2.4 - A.14.2.5 - A.14.2.6 - A.14.2.8 - A.14.2.9)
					Los administradores de las herramientas tecnológicas del Proceso Reparación Integral cada vez, generan mensajes de confirmación y validación frente a las transacciones (insertar, actualizar o eliminar) de información sobre el sistema de información. En caso de no confirmar la acción, la información no se actualizará. Como evidencia tenemos pantallazos de los sistemas de validación implementados en las herramientas. (A 12.4.1)			Atender a los requerimientos de la Oficina de Tecnologías de la información frente a los planes de mejoramiento de seguridad de la información cuando sea requerido el proceso. (A.18.2.2 - A.14)
					Los administradores de las herramientas tecnológicas del Proceso Reparación Integral cuentan con monitoreos mensuales de las fechas y horas de ingreso a las herramientas que permiten identificar los accesos de los usuarios a las herramientas, donde se busca identificar casos inusuales. En caso de ingresos sospechosos se realiza el bloqueo de los usuarios y se adelanta la investigación. Como evidencia tenemos los informes mensuales de seguimiento de los aplicativos. (A 12.4.1 - A 12.4.2 - A 12.4.3)			Promover el etiquetado de información con Enterprise Mobility Security (EMS) de Microsoft, aplicado a Word, Excel, PowerPoint y Access, herramienta que provee el Office 365 con el Windows 10. (A. 8.2.1 - A.8.2.2 - A.8.2.3)



Gestión De Talento Humano:

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Riesgo Inherente	Descripción del control	Riesgo Residual	Tratamiento	Plan de Acción
Administrar historias laborales y SIGEP	"Posibilidad de pérdida económica y reputacional ante los funcionarios de la Unidad por la pérdida total o parcial de la confidencialidad y/o integridad de la información almacenada en sistemas de información físico o digital considerado crítico, debido a la divulgación, pérdida y/o alteración de la información personal y/o laboral de los funcionarios activos y/o retirados de la Unidad.	Muy Baja	Mayor	Alto	El funcionario responsable de las historias laborales diligencia a diario los registros para el control de la custodia y contenido de los expedientes, identificando fecha, responsable, contenido y folios de los documentos manipulados. En caso de identificar faltantes o alteraciones requerirá formalmente al último responsable registrado e informará a la Coordinación de Talento Humano las demoras o inconsistencias en las respuestas para que se adelanten las investigaciones pertinentes. Evidencia: Formato préstamo de documentos (710.14,15-13) y Formato hoja de control de expedientes de historias laborales (710.14.15-33) (A.9.2.2 - A.9.2.3 - A.9.3)	Alto	Reducir - Mitigación	Implementar herramienta tecnológica que permita la digitalización de las historia laborales, esto permite reducir a manipulación de la historias laborales de los funcionarios y a su vez el riesgo de pérdida de los documentos.  (A.14.1.1)
					El grupo de Gestión administrativa y documental presta el apoyo diariamente a la custodia de los expedientes laborales de los funcionarios de la Unidad, El grupo de Talento Humano una vez se cuente con la documentación completa por cada expediente laboral, entrega los expedientes para custodia, el Grupo de gestión Administrativa realiza la recepción del documentación, realizando el check list respectivo por cada historia laboral, en los que casos que la documentación se encuentre incompleta el funcionario del Grupo de gestión administrativa procede a devolver todo el expediente laboral para revisión y ajuste por parte del Grupo de gestión de Talento Humano, Evidencia: Formato listado de requisitos(770,12,15-61), Formato hoja de control de expedientes de historias laborales (710.14.15-33). (A.9.2.2 - A.9.2.3 - A.9.3)			Implementar módulo de hojas de vida en la herramienta tecnológica de administración de planta de Talento Humano que fortalezcan la administración y control de historias laborales.  (A.14.1.1)
								Realizar capacitación al personal de Talento Humano que gestiona y custodia los expedientes laborales de los funcionarios de la Unidad, sobre el manejo de los expedientes y disposición de los mismos. (A.7.1)



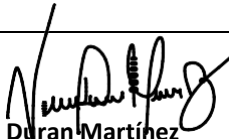


### Gestión Financiera

Actividad	Redacción del riesgo	Probabilidad Inherente	Impacto Inherente	Riesgo Inherente	Descripción del control	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 cómputo.	Muy Alta	Moderada	Alto	<p>La persona delegada como administrador del aplicativo "Sistema Integral de Información Financiera -SIIF Nación; tramita la solicitud de usuario que le permita el acceso a la información a través de un usuario asignado por Min hacienda. Como evidencia se cuenta con el formato diligenciado y los soportes requeridos, y autorización de acceso a las herramientas, o correos de solicitud de usuario. (A.9.2 - A.9.2.1 - A.9.2.2)</p> <p>Personal administrativo de la gestión Financiera, 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 evidencias se cuenta con los acuerdos de confidencialidad suscritos por cada herramienta en el OneDrive. (A.13.2.4)</p>	Moderado	Reducir - Mitigación	<p>Correos de incidencias y solicitudes de apoyo a la mesa de ayuda de Min hacienda</p> <p>(A.16.1.2 - A.16.1.5)</p>
Control y registro de información financiera en SIIF NACION II. Mediante Firma Digital	Posibilidad de pérdida económica y reputacional por acceso no autorizado, 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	<p>La persona delegada como administrador de 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. 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)</p> <p>La persona delegada como administrador de las firmas certificadas, trimestralmente, debe validar la necesidad de las firmas digitales y reportar a la Coordinación del Grupo de Gestión Financiera y Contable las fechas de vencimiento del dispositivo o token asignado, por medio de contrato vigente. 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)</p>	Moderado	Reducir - Mitigación	<p>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</p> <p>(A.10.1.2)</p>

CONTROL DE CAMBIOS

Versión	Fecha del cambio	Descripción de la modificación
1	Junio 2018	Creación documento plan de tratamiento de riesgos.
2	Agosto 2019	Actualización del mapa de riesgos 2019
3	Octubre 2020	Actualización del mapa de riesgos 2020
4	Diciembre 2021	Actualización del mapa de riesgos 2021
5	Enero 2022	Actualización del Plan de Tratamiento de Riesgo por actualización y publicación del mapa de riesgos vigencia 2022 y ajuste en el control de cambios de la versión 4.

<b>Proyectado por:</b> Helena Patricia Moreno Durán   <b>Revisado:</b> Joaquín Rojas Palomino  Enero 2022	<b>Aprobado:</b>  Víctor Edgardo Durán Martínez
--	--