2026

PSPSI
Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información.

Versión 01 Enero 2026

Ministerio de Defensa Nacional

Dirección de Veteranos y Rehabilitación Inclusiva - DIVRI

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.

TABLA DE CONTENIDO

Contenido

INTRODUCCION 3

1. OBJETIVO 4

2. ALCANCE 4

3. DEFINICIONES 4

4. MARCO NORMATIVO 5

5. TRATAMIENTO DE RIESGOS 5

6. RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA ENTIDAD 6

7. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 8

8. PROYECCION DE PRESUPUESTO CUMPLIMIENTO PLAN DE TRATAMIENTO DE RIESGOS 11

INTRODUCCION

Mediante la definición del Plan de Tratamiento de Riesgos se busca mitigar los riesgos presentes en el análisis de riesgos (Perdida de la Confidencialidad de los activos, Perdida de Integridad de los activos y Perdida de Disponibilidad de los activos) evitando aquellas situaciones que impidan el logro de los objetivos del DIVRI.

Este Plan de Tratamiento de Riesgo se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes, estas acciones son organizadas en forma de medias de seguridad, y para cada una de ellas se define el nombre de la medida, objetivo, justificación, responsable de la medida y su prioridad.

Este plan busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos, dando a conocer aquellas situaciones que pueden afectar el cumplimiento de los objetivos estratégicos, a partir de la alineación al modelo de seguridad y privacidad de la información de la DIVRI.

1. OBJETIVO

Establecer una metodología que permita la gestión del riesgo de seguridad de la información basado en los criterios de Confidencialidad, Integridad y isponibilidad, que permitan la protección de los activos de información de la DIVRI.

1.2 Objetivos Específicos

Realizar la identificación y tratamiento de los riesgos para reducir el impacto ante la ocurrencia de eventos de seguridad de la información.

Fortalecer y apropiar el conocimiento referente a la gestión de riesgos de Seguridad y Privacidad de la información.

2. ALCANCE

Comprende las acciones que deben tomar las diferentes áreas de la entidad en el tratamiento de riesgos de seguridad y privacidad de la información con base en los lineamientos definidos en las políticas y tiempos definidos en el Plan de Seguridad y Privacidad de la Información.

3. DEFINICIONES

Amenaza. Es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

Control o Medida. Acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

Impacto. Son las consecuencias que genera un riesgo una vez se materialice.

Probabilidad. Es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.

Riesgo. Es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.

Vulnerabilidad. Es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

4. MARCO NORMATIVO

Decreto 1008 de 2018. Establece los lineamientos generales de la política de Gobierno Digital. Deroga el Decreto 2573 de 2014.

Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

NTC / ISO 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).

Guía No. 7. Guía de gestión del riesgo, versión 3.0 – del Ministerio de Tecnologías de la Información y las Comunicaciones.

5. TRATAMIENTO DE RIESGOS

El tratamiento de riesgos es la respuesta establecida por la primera línea de defensa, es decir, el líder o responsable del proceso junto con su equipo de trabajo para la mitigación de los diferentes riesgos.

El propósito del tratamiento del riesgo es seleccionar e implementar opciones para abordar el riesgo, y debe implicar un proceso iterativo de:

- Formular y seleccionar opciones para el tratamiento del riesgo
- Planificar e implementar el tratamiento del riesgo
- Evaluar la eficacia de ese tratamiento
- Decidir si el riesgo residual es aceptable
- Si no es aceptable, efectuar el tratamiento adicional.

La política de Administración de Riesgo establece las opciones para tratar los riesgos residuales ya sea fortaleciendo los actuales controles o implementado nuevos controles, para lo cual deberá tener en cuenta las siguientes opciones de manejo:

Evitar el riesgo. Corresponde tomar medidas encaminadas a prevenir o eliminar las causas para su materialización u ocurrencia. Es siempre la primera alternativa a considerar y se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño, eliminación de la actividad que causa el riesgo, y como resultado de unos adecuados

controles y acciones emprendidas. Un ejemplo de esto puede ser el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, entre otros. Aceptar el riesgo. Corresponde a asumir las consecuencias del riesgo por considerar de muy baja probabilidad su ocurrencia y de leves consecuencias, o en su defecto, luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se acepta la pérdida en caso de materialización. Se elaboran planes de contingencia para su manejo.

Reducir el riesgo. Corresponde tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), sus impactos (medidas de protección), o ambas. La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Se consigue mediante la optimización de los procedimientos y la implementación de controles.

Compartir el riesgo. Se reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, mediante un contrato determinado, como en el caso de los contratos de seguros, tercerización o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Es así como, por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar.

6. RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA ENTIDAD

La DIVRI, Se encuentran realizando la definición del formato MAPA Y PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL, donde se consagra todo lo relacionado a la implementación del plan de tratamiento de riesgos y privacidad de la información de la ENTIDAD.

Para la vigencia 2024, se establecen e identifican los siguientes riesgos:

Proceso	Referencia	Activo de Información	Tipo de activo	Amenazas (Causa Inmediata)	Vulnerabilidades (Causa raiz)	Tipo de riesgo	Descripción del Riesgo	Clasificación riesgo
Rehabilitacion Inclusiva	1	Sistema de informacion Misioanl de Rehabilitacion Inclusiva - SIMRI	Software	Incumplimiento en el soporte y mantenimiento del sistema de información.	Ausencia o insuficiencia de pruebas de software	Perdidad de Disponibilidad	Perdida de la disponibilidad del sistema de informacion, debido a la implementacion de los nuevos desarrollos o mejoras que afectan opciones o reglas de negocio configuradas en el sistema de informacion	Fallas tecnológicas
TICS	2	Equipos informaticos	Hardware	Polvo, corrosión, Congelamiento	mantenimiento insuficiente	Perdidad de Disponibilidad	Perdida de la disponibilidad de la información debido a dano fisico o fallas técnicas en los dispositivos tecnológicos (hardware)	Fallas tecnológicas
Prestaciones Sociales	3	Software de liquidacion Nomina Paoyer de nomina	Software	Falsificación de derechos	Autenticación debil	Perdidad de integridad	Perdida de integridad por la autenticación de un usuario no autorizado debido a una autenticación debil en el software de gestion de nomina, que utiliza un unico factor de autenticación como es: usuario y contraseña y que permite a un usuario interno realizar modificaciones no permitidas	Fraude interno
Prestaciones Sociales	4	Carpeta compartida "Nomina"en One Drive	informacion	Error en el uso Falta de conciencia acerca de la seguridad	Autenticación debil	Perdidad de integridad	Perdida de integridad por la manipulacion y acceso a la carpeta nomina, la cual contiene informacion de vigencias del 2004-2020, y no organizada	Fraude interno
TICS	5	Archivo liqui	informacion	Manipulacion con sofware	compromiso de la informacion	Perdidad de integridad	Perdida de integridad por la manipulacion del archoivo liqui, el cual por su tamaño se debe manipular y parttir en doce archivos para subir la informacion a la pagina web	Fraude interno
TICS	6	Red de Datos Locales	red	Mal funcionamiento del software	Conexión deficiente del cableado	Perdidad de Disponibilidad	Perdida de disponibilidad por fallas en la comunicación entre los servidores de aplicaciones y los equipos de usuarios finales, y dificultades en el mantenimiento y accesibilidad a la estructura del cableado de datos.	Fallas tecnológicas

7. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016)2, bajo la responsabilidad del proceso TIC de la DIVRI.

Riesgos identificados (agrupados):

1. Acceso no autorizado / Robo de credenciales / Suplantación de identidad
2. Pérdida de datos por fallos, ataques o errores humanos
3. Intercepción de datos / Ataques Man-in-the-Middle / Fuga de información
4. Exposición de datos sensibles / Exfiltración de información crítica
5. Infección por malware, ransomware, spyware
6. Caídas del sistema / Indisponibilidad del servicio
7. Incidentes o riesgos no detectados (falta de monitoreo)

Actividades de tratamiento por riesgo:

Riesgo	Actividades de tratamiento	Responsable sugerido	Tiempo estimado
Acceso no autorizado / Robo de credenciales / Suplantación de identidad -RUM	Implementar MFA, al sistema de información RUM.	Equipo TIC	01/02/2026 AL 30/06/2026
	Copias de seguridad con pruebas de restauración	Equipo TIC	01/02/2026 AL 30/06/2026
Pérdida de datos por fallos, ataques o errores humanos – Directorio Activo	Fortalecer la seguridad y la gestión de identidades mediante la migración del servicio de Directorio Activo desde el hardware obsoleto hacia un nuevo servidor con soporte vigente, garantizando la eliminación de vulnerabilidades por falta de	Equipo TIC	30/06/2026 al 31/12/2026

	parches y asegurando la disponibilidad del servicio.		
Infección por malware, ransomware, spyware	Implementar procesos de ingesta y escaneo de vulnerabilidades en coordinación con el CSIRT institucional, con el fin de fortalecer la seguridad de la infraestructura tecnológica y garantizar la detección temprana de riesgos	Equipo TIC	01/03/2026 al 31/12/2026

Proceso	Referencia	Activo de Información	Tratamiento	Plan de Acción	Responsable	Fecha de Implementación	Seguimiento	Estado
Rehabilitacion Inclusiva	1	Sistema de información Misional de Rehabilitación Inclusiva - SIMRI	Reducir	implementar los ambientes de pruebas y desarrollo en la nube publica de la DIVRI	TICS	31/03/2025	semestral	incial
TICS	2	Equipos informaticos	Reducir	implementar servicios de mesa de ayuda para la infraestructura tecnológica de la Entidad	TICS	31/03/2026	semestral	incial

Prestaciones Sociales	4	Carpeta compartida "Nomina"en One Drive	Reducir	organizar las carpetas por vigencias. De acuerdo a las tablas de retención y definir los perfiles de lectura y escritura de los usuarios que requieren la informacion	prestaciones sociales	31/10/2025	semestral	incial
TICS	5	Archivo liqui	Reducir	Crear un desarrollo de software que impida la manipulación del archivo liqui,	TICS	31/10/2025	semestral	incial
TICS	6	Red de Datos Locales	Reducir	realizar el contrato para mantenimiento preventivo y correctivo de redes de datos	TICS	31/10/2026	semestral	inicial

8. PROYECCION DE PRESUPUESTO CUMPLIMIENTO PLAN DE TRATAMIENTO DE RIESGOS

A continuación, se presentan las actividades y la proyección presupuestal para cumplir con dicha actividad:

PRESUPUESTO 2026	
SERVICIO INFRAESTRUCTURA TECNOLOGICA	**VALOR**
Soporte y Mantenimiento Software	720.000.000
Renovación de Licencias Software	600.000.000
Redes y seguridad	130,000,000
Conectividad	400,000,000
Mantenimiento Preventivo y Correctivo	100.000.000
TOTAL	1.950.000.000