UNGRD
Unidad Nacional para la Gestión del Riesgo de Desastres

Plan de Tratamiento de Riesgos

Grupo de Tecnologías de la Información.

Enero 2026

Contenido

TABLAS

RESUMEN EJECUTIVO

El Plan de Tratamiento de Riesgos de Seguridad de la Información de la UNGRD establece las acciones, responsables, plazos y evidencias requeridas para tratar los riesgos identificados en el marco del Sistema de Gestión de Seguridad de la Información (SGSI), de acuerdo con los criterios de aceptación del riesgo definidos por la Entidad. Su alcance aplica a todos los procesos y colaboradores, e integra la priorización de riesgos conforme a su nivel inherente y residual, con énfasis en aquellos ubicados en niveles "Alto" y "Extremo".

El Plan consolida el tratamiento mediante la definición de controles existentes y acciones de mejora, alineadas con buenas prácticas y lineamientos de ISO/IEC 27001:2013, ISO 31000:2018 y la guía del DAFP para administración del riesgo y diseño de controles en entidades públicas. Para cada riesgo priorizado se especifica el control asociado (Anexo A), la evidencia/soporte, el responsable (dueño del riesgo y áreas de apoyo), y la fecha de implementación, garantizando un enfoque documentado, sistemático y verificable.

INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad de la Información tiene como propósito evaluar y definir las acciones necesarias para mitigar los riesgos identificados, conforme a los criterios de aceptación del riesgo establecidos por la Entidad. Estas acciones deben ser conocidas, gestionadas y ejecutadas de manera documentada, sistemática, estructurada y eficiente.

Contar con una visión integral de los riesgos que pueden afectar la seguridad de la información permite a la Entidad establecer controles y medidas efectivas, viables y transversales, orientadas a preservar la confidencialidad, integridad y disponibilidad de la información. En este marco, se hace necesario definir los lineamientos para el análisis y la evaluación de los riesgos de Seguridad de la Información en la Entidad.

Lo anterior se desarrolla en cumplimiento de la normativa aplicable en el Estado colombiano, adoptando buenas prácticas y lineamientos de los estándares ISO/IEC 27001:2013, ISO 31000:2018 y de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas emitida por el DAFP.

TÉRMINO Y DEFINICIONES

Activo de información: aquello que es de alta validez y que contiene información vital de la Entidad que debe ser protegida.

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 Entidad (materializar el riesgo).

Asumir/Aceptar: La entidad acepta el riesgo en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección y lo asume conociendo los efectos de su posible materialización.

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.

Evaluación de riesgo: Proceso de comparar los resultados del análisis de riesgo con los criterios de riesgo para determinar si el riesgo y / o su magnitud es aceptable o tolerable. La evaluación de riesgos ayuda en la decisión sobre el tratamiento de riesgos.

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.

Reducir/Mitigar: El riesgo se trata mediante la transferencia o la implementación de acciones que mitiguen su nivel. No necesariamente es un control adicional.

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

Seguridad de la Información: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la

información de las entidades del Estado, y de los servicios que prestan al ciudadano.

Control: Medida que permite reducir o mitigar un riesgo.

OBJETIVO

Objetivo General

Detallar el Plan de Tratamiento de Riesgos que hace parte del Sistema de Gestión de Seguridad de la Información (SGSI) de la Unidad Nacional para la Gestión del Riesgo de Desastres (UNGRD), mediante el cual se establecen los controles y acciones orientados a tratar y mitigar los riesgos de seguridad de la información, reduciendo la probabilidad de su materialización y/o su impacto

Objetivos específicos

- ✓ Identificar los riesgos de seguridad de la información asociados a los procesos y activos de información incluidos en el alcance del SGSI.
- ✓ Analizar y valorar los riesgos identificados para determinar su nivel (probabilidad, impacto y zona de riesgo).
- ✓ Definir y documentar el Plan de Tratamiento de Riesgos, estableciendo controles, responsables, plazos y evidencias.
- ✓ Realizar seguimiento y evaluación a la implementación y efectividad del Plan de Tratamiento de Riesgos, promoviendo acciones de mejora cuando corresponda.
- ✓

ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad de la Información es aplicable a todos los procesos de la UNGRD y a los colaboradores de todos los niveles. Comprende desde la identificación de los riesgos de seguridad de la información clasificados en niveles "Alto" y "Extremo" en la Matriz de Riesgos de Seguridad de la Información, hasta la definición del plan de tratamiento, incluyendo controles, responsables y fechas de implementación.

METODOLOGÍA

Teniendo en consideración la GUÍA METODOLÓGICA GESTIÓN DE RIESGOS PARA SGSI (G-1101-GTI-01) de la entidad, en la definición del Plan de tratamiento de riesgos de seguridad de la información se realizaron las siguientes actividades en conjunto con los colaboradores asignados para cada proceso de la entidad:

1. Identificación de los riesgos residuales: Se identifican los riesgos que están en la zona del riesgo residual alto o extremo.

2. Opción de tratamiento: Campo que se calcula automáticamente de acuerdo con la valoración del riesgo residual, según la zona donde se ubica el riesgo residual, se determina la opción o estrategia de tratamiento a seguir para combatir el riesgo, para esta actividad se debe considerar la siguiente tabla:

ZONA DE RIESGO RESIDUAL	NIVEL DE RIESGO ACEPTABLE	OPCIÓN O ESTRATEGIA DE TRATAMIENTO A SEGUIR
Bajo	**Aceptable**	**Asumir/Aceptar**
Moderado	**Aceptable**	**Asumir/Aceptar**
Alto	**No Aceptable**	**Reducir/Mitigar**
Extremo	**No Aceptable**	**Reducir/Mitigar**

Tabla 1. Zona de Riesgo Residual

3. Acciones de mejora: Es la redacción del control teniendo en cuenta la siguiente estructura; responsable de la ejecución + acción realizada + complemento.

4. Control Anexo A de la NTC-ISO-IEC 27001:2013: Seleccionar de la lista desplegable.

5. Soporte: Registro de la evidencia que deja la implementación de la acción de mejora.

6. Responsable: Registrar el rol o cargo responsable de implementar la acción de mejora.

7. Fecha implementación: Periodo de tiempo en el cual se implementará la acción de mejora.

Resultado valoración de Riesgos de Seguridad de la Información

La identificación y valoración de riesgos sobre los activos de información de la entidad se encuentra detallada en la Matriz de Gestión de Riesgos de Seguridad de la Información cargada en NEOGESTION (RG-1101-GTI-04).

A continuación, se discriminan los riesgos de seguridad de la información identificados por nivel de riesgo residual:

vel del Riesgo	Cantidad de Riesgos	Porcentaje%
Bajo	23	54,76%
Moderado	15	35,72%
Alto	2	4,76%
Extremo	2	4,76%
TOTAL	42	100%

Tabla 2. Valoración Riesgo Residual

Si el riesgo se ubica en una zona no aceptable, cada líder responsable de los riesgos identificados con el apoyo del Grupo de Tecnologías de la Información, debe definir e implementar los controles necesarios para llevar el riesgo a un nivel aceptable a través del plan de tratamiento de riesgos. Se establecieron las siguientes acciones de mejora para abordar los cuatro (4) riesgos en valoraciones alta y extrema:

IDENTIFICACION DEL RIESGO					ZONA DE RIESGO RESIDUAL	PLAN DE TRATAMIENTO					
ID	PROCESO	TIPO DE ACTIVO DE INFORMACIÓN	RIESGO	DESCRIPCIÓN DEL RIESGO		OPCIÓN DE TRATAMIENTO	ACCIONES DE MEJORA	CONTROL ANEXO A NTC-ISO- IEC 27001:2013	SOPORTE	RESPONSABLE	Fecha implementación
18	Gestión de tecnologías de la información	Hardware	Confidencialidad	Afectación reputacional y legal por ataque informático debido a desconocimiento de las políticas para el buen uso de los activos de información (Red, Correo, Internet, Sistemas de Información, Chat, Redes Sociales, etc.) por parte de los colaboradores.	**Extremo**	Reducir/Mitigar	Simulaciones de ejercicios de ingeniería social.	A.7.2.2-Toma de conciencia, educación y formación en la seguridad de la información	informe de resultados plan de refuerzo/capacitación focalizada.	Líder del proceso y proveedor	Primer semestre
31	Servicio al ciudadano	Software	Confidencialidad	Posibilidad de abuso de privilegios debido a asignación errada de los mismos.	**Alto**	Reducir/Mitigar	Solicitar periódicamente al Grupo de Tecnologías de la Información la revisión y actualización de los accesos del Sistema PQRSD, verificando que los usuarios, roles y privilegios	A.9.2.5-Revisión de los derechos de acceso de usuarios	Informe/acta de revisión de accesos del PQRSD y ticket o radicado de solicitud a GTI.	Líder del proceso de Servicio al ciudadano con apoyo del Grupo de tecnologías de la información	A demanda
53	Gestión de Control Disciplinario	Recurso Humano	Disponibilidad	Ausencia de personal de planta o contratistas conlleva a que no se cumplan con los objetivos del proceso de control disciplinario	**Extremo**	Reducir/Mitigar	Solicitar la contratación de un abogado con experiencia en derecho disciplinario o afines	A.9.2.5-Revisión de los derechos de acceso de usuarios	Documentos precontractuales correspondientes	Líder del proceso	Primer cuatrimestre
55	Gestión de tecnologías de la información	Hardware	Disponibilidad	Indisponibilidad de servicios internos y/o externos por falla del almacenamiento central que soporta VMs, FileServer y portales institucionales.	**Alto**	Reducir/Mitigar	Evaluar y documentar alternativas para garantizar disponibilidad del storage/backup (redundancia/separación/externo/punto unico de falla) y ejecutar plan de mitigación con monitoreo, retención validada.	A.12.1.3 – Gestión de la capacidad A.12.4.1 Registro de eventos (para trazabilidad/alertas)	Informe con presentación de las alternativas para mitigación del riesgo.	Líder del proceso	Primer semestre

Tabla 3. Plan Acciones de Mejora

DOCUMENTOS ASOCIADOS

- Decreto 612 de 4 de abril de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.
- Decreto 1008 de 14 de junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.
- RG-1300-SIPG-84 Política de Administración de Riesgos de la UNGRD.
- RG-1101-GTI-04 Matriz de Riesgos de Seguridad de la Información
- G-1101-GTI-01 Guía Metodológica Gestión de Riesgos para SGSI
- Plan de tratamiento de riesgos 2025 UNGRD
- Plan tratamiento de Riesgos de seguridad y privacidad de la información versión 7 2025 - MINTIC

CONTROL DE CAMBIOS

Fecha	Versión	Descripción del cambio
16/01/2026	1	Emisión inicial

Elaboro: Carlos Andrés Granados Guevara / Oficial de Seguridad de la Información / Contratista
Aprobó: Comité Institucional de Gestión y Desempeño (xx/xx/xxxx)