1. TABLA DE CONTENIDO

1. TABLA DE CONTENIDO....1
2. INTRODUCCIÓN....1
3. OBJETIVOS....1
4. ALCANCE....2
5. DEFINICIONES....2
6. REQUERIMIENTOS LEGALES Y OTROS REQUISITOS....3
7. METODOLOGIA....3
8. PLAN DE TRATAMIENTO DE RIESGOS DE SEGUIRDAD DE LA INFORMACION....6
9. CONTROL DE CAMBIOS DEL DOCUMENTO....7

2. 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 27001:2022, ISO 31000:2018 y de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas emitida por el DAFP.

3. OBJETIVOS

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.

4. 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.

5. DEFINICIONES

Activo de información: Aquello que es de alta validez y que contiene información vital de la Entidad que debe ser protegida. (Modelo de Seguridad y Privacidad de la Información MSPI - MinTIC, 2018)

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. (Guía para la Administración del Riesgo - Función Pública, 2018)

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. (Guía para la Administración del Riesgo - Función Pública, 2018)

Impacto: Son las consecuencias que genera un riesgo una vez se materialice. (Modelo de Seguridad y Privacidad de la Información MSPI - MinTIC, 2018)

Probabilidad: Es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo. (Modelo de Seguridad y Privacidad de la Información MSPI - MinTIC, 2018)

Reducir/Mitigar: El riesgo se trata mediante la transferencia o la implementación de acciones que mitiguen su nivel. No necesariamente es un control adicional. (Guía para la Administración del Riesgo - Función Pública, 2018)

Riesgo: Es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos. (Modelo de Seguridad y Privacidad de la Información MSPI - MinTIC, 2018)

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. (Decreto 1008 Presidencia de la República, 2018)

6. REQUERIMIENTOS LEGALES Y OTROS REQUISITOS

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 27001:2022 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

7. METODOLOGIA

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:

Tabla 1. Zona de Riesgo Residual

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**

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 27001:2022**: 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.

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

Tabla 2. Valoración Riesgo Residual

Nivel 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%

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:

8. PLAN DE TRATAMIENTO DE RIESGOS DE SEGUIRDAD DE LA INFORMACION

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 27001:2022	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 c olaboradores.	**Extremo**	Reducir/Mitigar	Simulaciones de ejercicios de ingeniería social.	A.7.2.2-Toma de conciencia, educación y formaciónen la seguridad de la información	informe de resultados plan de refuerzo/capacitación focalizada.	Líder del Proceso y OSI	Segundo 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 asignados correspondan a las funciones autorizadas.	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 y OSI	A demanda
53	Gestión de Control Disciplina	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 suarios	Documentos precontract uales correspondi entes	Líder d el proceso	Segundo semestre
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	Finalizar implementación para garantizar disponibilidad del storage/backup (redundancia/separación/extern o/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 los resultados de implementación	Líder del proceso	Segundo semestre

9. CONTROL DE CAMBIOS DEL DOCUMENTO

VERSIÓN	DESCRIPCIÓN DEL CAMBIO	FECHA
01	Emisión Inicial	16/01/2026
02	Se realizó la actualización integral del Plan de Tratamiento de Riesgos de Seguridad de la Información para la vigencia 2026, revisando y ajustando las actividades asociadas a los riesgos clasificados en niveles Alto y Extremo. Se actualizaron las fechas de ejecución e implementación de las acciones de mejora establecidas en los planes de tratamiento, garantizando su alineación con la programación institucional vigente. Adicionalmente, se revisaron los responsables definidos para la ejecución y seguimiento de las actividades, efectuando los ajustes requeridos según la estructura operativa actual.	08/07/2026

ELABORÓ	REVISÓ	APROBÓ
Nombre: Pedro Elías Ballesteros Peñaranda	**Nombre:** Iván Dario Huertas Perdomo	**Nombre:** Isabel Cristina Arboleda López
Cargo: Contratista FNGRD	**Cargo:** Profesional Especializado	**Cargo:** Coordinadora GTI (E)