



GOBIERNO DE COLOMBIA



Sistema Nacional de Gestión del Riesgo de Desastres

# PLAN DE TRATAMIENTO DE RIESGOS 2023

Grupo de Tecnologías de la Información.

27 de enero del 2023.



# Contenido

1. Introducción.....	3
2. Términos y Definiciones .....	3
3. Objetivo.....	4
3.1 Objetivo General .....	4
3.2 Objetivos específicos .....	4
4. Alcance .....	5
5. Metodología .....	5
5.1 Resultado valoración de Riesgos de Seguridad de la Información .....	6
5.2 Acciones para el tratamiento de riesgos.....	6
6. Recomendaciones.....	8
7. Documentos Asociados.....	8
8. Control de cambios .....	8



# 1. Introducción

El objetivo fundamental del Plan de tratamiento de riesgos de Seguridad de la Información, es evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes teniendo en cuenta los criterios de aceptación de riesgos definidos por la Entidad. Dichas acciones deben ser conocidas, tratadas y ejecutadas por la Entidad de una forma documentada, sistemática, estructurada y eficiente.

En la medida que se tenga una visión de los riesgos que pueden afectar la seguridad de la información, la Entidad puede establecer controles y medidas efectivas, viables y transversales, con el propósito de preservar la disponibilidad, integridad y confidencialidad de su información, para lo cual es necesario definir los lineamientos que se deben seguir para el análisis y evaluación de los riesgos de Seguridad de la Información de la Entidad.

Lo anterior dando cumplimiento a la normativa establecida por el estado colombiano y adoptando las buenas prácticas y los lineamientos de los estándares ISO/IEC 27001:2013, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas emitida por el DAFP.

## 2. Términos 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.

## 3. Objetivo

### 3.1 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, mediante el cual se definen los controles que permiten mitigar la materialización de los riesgos de seguridad de la información en la UNGRD.

### 3.2 Objetivos específicos

- Identificar los riesgos asociados a los procesos y los activos de información que hacen parte del alcance del SGSI
- Calcular el nivel de riesgo
- Establecer el plan de tratamiento de riesgos
- Realizar seguimiento y control a la eficacia del plan de tratamiento de riesgos

## 4. Alcance

El Plan de tratamiento de riesgos de seguridad de la información es aplicable a todos los procesos de la UNGRD, con alcance a los colaboradores de todos los niveles; desde la identificación de los riesgos de seguridad de la información que se encuentran en los niveles “Alto” y “Extremo” en la Matriz de riesgos de Seguridad de la Información de la UNGRD hasta la definición del plan de tratamiento, responsables y fechas de implementación.

## 5. 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:

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

**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

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

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

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

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



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

## 5.1 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 (RG-1101-GTI-04).

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

Nivel del Riesgo	Cantidad de Riesgos	Porcentaje%
<b>Bajo</b>	23	63,89%
<b>Moderado</b>	10	27,78%
<b>Alto</b>	1	2,78%
<b>Extremo</b>	2	5,56%
<b>TOTAL</b>	36	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. A continuación, se definen las siguientes estrategias de tratamiento, asumir los riesgos bajos y moderados y gestionar el riesgo alto y extremo. A continuación, se muestra la estrategia para abordar los tres (3) riesgos y establecer su tratamiento:

## 5.2 Acciones para el tratamiento de riesgos

Los responsables de los activos de información deben contribuir con el seguimiento y control los riesgos identificados, además de la implementación de las acciones definidas en el presente plan de tratamiento. Por lo tanto, la estimación y asignación de los recursos requeridos, corresponderá al responsable del activo.

IDENTIFICACIÓN DEL RIESGO VALORACIÓN DEL RIESGO RESIDUAL					PLAN DE TRATAMIENTO						
ID DEL RIESGO	PROCESO	CATEGORIA/TIPO DE ACTIVO DE INFORMACIÓN	NOMBRE DEL RIESGO	DESCRIPCIÓN DEL RIESGO	ZONA DE RIESGO RESIDUAL	OPCIÓN DE TRATAMIENTO	ACCIONES DE MEJORA	CONTROL ANEXO A NTC-ISO-IEC 27001:2013	SOPORTE	RESPONSABLE	FECHA IMPLEMENTACION
37	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.7.1.1 Selección	Documentos precontractuales correspondientes	Operador disciplinario	Primer cuatrimestre
18	Grupo de Tecnologías de la Información	Información	Disponibilidad	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	Fortalecer las capacitaciones y sensibilizaciones al personal del proceso en cuanto a la importancia de seguridad y el uso adecuado de los activos de información tales como el drive (repositorio documental)	A.7.2.2-Toma de conciencia, educación y formación en la seguridad de la información	Registros definidos para las actividades a realizar (listas de asistencia, grabación, videos, piezas gráficas, etc.)	Líder del proceso y grupo de tecnologías de la información	Según cronograma actividades de Sensibilización (PETI)
31	Servicio al Ciudadano	Software	Confidencialidad	Posibilidad de abuso de privilegios debido a asignación errada de los mismos.	Alto	Reducir/Mitigar	Solicitar al Grupo de tecnologías de la información la revisión periódica de los controles de acceso y privilegios del personal del proceso y realizar seguimiento a su cumplimiento	A.9.2.5-Revisión de los derechos de acceso de usuarios	Informe de revisiones	Grupo de tecnologías de la información y el Líder del proceso de Servicio al ciudadano	Cuatrimstral



## 6. Recomendaciones

- Involucrar a los diferentes procesos de la entidad en la identificación, valoración, control y monitoreo de riesgos de seguridad de la información.
- Realizar seguimiento periódico a los controles y plan de tratamiento según lo establecido en la metodología y directrices aprobadas para la gestión de riesgos de seguridad de la información.
- Identificar oportunidades, entendiendo oportunidad como la consecuencia positiva frente al resultado del tratamiento del Riesgo.

## 7. 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 2022 UNGRD
- Plan tratamiento de Riesgos de seguridad y privacidad de la información versión 5 2023 - MINTIC

## 8. Control de cambios

Fecha	Versión	Descripción del cambio
27/01/2023	1	Elaboración del plan

*Elaborado por: Sylvia Ribero Corzo / Contratista GTI*

*Revisó: Carolina Jiménez Zapata / Coordinadora GTI*

