PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025

Agencia Nacional de Tierras

DIRECCIÓN DE GESTION DEL ORDENAMIENTO SOCIAL DE LA PROPIEDAD

SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN DE TIERRAS

Contenido

1. Introducción

Los procesos relacionados con seguridad de la información en la Agencia Nacional de Tierras, están basados en conceptos técnicos y operativos que bajo el conocimiento y la conciencia que tienen los colaboradores de la entidad, permitiendo que se asuma con responsabilidad las operaciones que estén asociadas a procesos tecnológicos, entendiendo que su uso puede conllevar a riesgos que exponen la infraestructura y los datos que son parte de los activos de información.

Ante este tipo de situaciones la entidad prepara y dispone una serie de controles, evaluaciones y acciones preventivas que conllevan al análisis de los riesgos, bajo la construcción y actualización del plan de tratamiento de riesgos, el cual, traza una hoja de ruta que oriente las acciones o procedimientos a desarrollar para mitigar la materialización del riesgo y la aparición de incidentes de seguridad.

2. Términos y definiciones

- Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

- Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

- Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

- Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

- Causa: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

- Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

- Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de

riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada. Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

- Disponibilidad: Propiedad que la información sea accesible y utilizable por solicitud de los autorizados (2.10 ISO 27000).

- Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

- Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

- Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

- Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- Identificación del riesgo. Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

- Impacto. Cambio adverso en el nivel de los objetivos del negocio logrados.

- Integridad: Propiedad de salvaguardar la exactitud y el estado completo de los activos (2.36 ISO 27000). Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

- Información: Conjunto de datos que tienen un significado.

- Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona de

riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

- Monitoreo: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de con trol o las diferentes auditorías de los sistemas integrados de gestión.

- Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

- Parte interesada: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

- Probabilidad: Posibilidad de que una amenaza se materialice.

- Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

- Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado.

- Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

- Reducción del riesgo. Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

- Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles. Riesgo Positivo: Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.

- Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

- Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera.

- Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

- Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

- Tratamiento del Riesgo: Proceso para modificar el riesgo" (Icontec Internacional, 2011).

- Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

- Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

3. Objetivos

3.1. Objetivo General:

Establecer las acciones requeridas para mitigar los riesgos de seguridad de la información mediante el Plan de Tratamiento de Riesgos, la implementación de controles y acciones preventivas que permitan mantener la integridad, disponibilidad y confidencialidad de los activos de información de la Agencia Nacional de Tierras.

3.2. Objetivos Específicos:

- Mejorar los mecanismos de identificación, evaluación tratamiento, monitoreo, mitigación y prevención de los riesgos, amenazas y vulnerabilidades asociados a seguridad de la información, mediante procesos documentales que permitan su ágil perfilación y controles que permita la protección de los recursos de TI.
- Actualizar y documentar los procedimientos y lineamientos requeridos para fortalecer la seguridad de la información en la entidad.
- Establecer un cronograma que permita el seguimiento a la ejecución de las acciones preventivas establecidas en cada dependencia, así como al desarrollo de controles.

- Tratar de manera integral los riesgos de seguridad de la Información.

- Cumplir con los requisitos legales y normativos colombianos sobre los riesgos en la seguridad de la información.

4. Alcance

El presente Plan de Tratamiento de Riesgos de seguridad de la información aplicará a la gestión de la mitigación de riesgos identificados en el año 2024 y la actualización de los mismos durante el año 2025, el mismo se desarrollará entre enero y diciembre de 2025, teniendo en cuenta que se han establecido acciones preventivas para aquellos riesgos en los cuales se han detectado controles en nivel débil y moderado.

5. Marco de referencia

5.1. Política de administración del Riesgo

La política de administración del riesgo (DEST-Politica-001 ADMINISTRACIÓN DEL RIESGO) tiene como finalidad establecer los lineamientos para la Administración de Riesgos en la Agencia Nacional de Tierras, a partir de los cuales se definirán los procedimientos y mecanismos de verificación y evaluación encaminados a la búsqueda de la eficiencia, eficacia y transparencia de los procesos.

5.2. Procedimiento de administración de riesgos de gestión

El procedimiento de administración de riesgos de gestión (DEST-P-001 ADMINISTRACION DE RIESGOS DE GESTION), permite determinar los fundamentos y las tareas para facilitar la evaluación y el tratamiento de los Riesgos de Gestión que pueden afectar el logro de los objetivos de procesos y planes establecidos por la Dirección General para el cumplimiento de las funciones asignadas a la Agencia Nacional de Tierras.

5.3. Política de seguridad y privacidad de la información

La política de seguridad y privacidad de la Información (NTI-Política-001 POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN) está comprometida con el tratamiento responsable de los activos de información utilizados a lo largo de las actividades incluidas dentro de cada uno de sus procesos, requeridos para consolidar y mantener el ordenamiento social de la propiedad rural y mejorar las condiciones de vida de la población.

Es por ello que la entidad está comprometida con la protección de la confidencialidad, integridad y disponibilidad de los diferentes activos de información (de tipo información, hardware, software, redes, servicios, procesos y personas), para lo cual mediante la adopción del Modelo de Seguridad de la Información implementado a través del Sistema de Gestión de Seguridad de la Información institucional que se encuentra alineado con el estándar ISO 27001, realiza la gestión

de riesgos de seguridad de la información y propende por la generación de cultura e implementación de buenas prácticas de seguridad de la información

5.4. Procedimiento para el Tratamiento de riesgos de seguridad de la información

El procedimiento (DEST–P-011 PROCEDIMIENTO ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN) determina los fundamentos y las tareas para facilitar la evaluación y el tratamiento de los Riesgos de Seguridad de la información que pueden afectar el Sistema de Gestión de Seguridad de la Información, así como el logro de los objetivos de seguridad establecidos por la Agencia Nacional de Tierras

5.5. Guía de gestión de riegos

Se adopta la Guía 7 de Gestión de Riesgos versión 3 de MinTIC, la cual permite a las entidades gestionar los riesgos de Seguridad de la información, basado en los criterios de seguridad (Confidencialidad, Integridad, Disponibilidad) buscando la integración con la Metodología de riesgos del DAFP, logrando vincular la identificación y análisis de Riesgos de la Entidad hacia los temas de la Seguridad de la Información.

5.6. Guía para la administración de riesgos – DAFP

La guía para la administración del riesgo armoniza el Modelo Estándar de Control Interno (MECI) y la Norma Técnica de Calidad NTCGP1000:2009, facilita a las entidades el ejercicio de la administración del riesgo. Cabe anotar que el ICONTEC a través de la norma NTC-ISO 31000 actualizó la norma NTC5254.

6. Metodología

El Departamento Administrativo de la Función Pública – DAFP actualizó en noviembre de 2022 la “Guía para la administración del riesgo y el diseño de controles en entidades públicas”, unificando una metodología para administrar de manera efectiva los riesgos de corrupción, gestión, fiscal y seguridad digital en las Entidades públicas. Adicionalmente esta guía incluye la evaluación de los controles definidos para mitigar los riesgos con el fin de determinar su efectividad de manera objetiva y define un esquema de líneas de defensa, estableciendo roles y responsabilidades del personal involucrado en la gestión de riesgos.

Tomando como referencia la documentación mencionada, la Agencia Nacional de Tierras actualizó la Política de Seguridad y Privacidad de la información y creo el Procedimiento para la administración de riesgos de Seguridad de la Información estableciendo los lineamientos para la identificación, análisis, evaluación, tratamiento, monitoreo, revisión y seguimiento de los riesgos de Seguridad de la información, buscando prevenir de forma anticipada su ocurrencia y minimizar el impacto que pueda afectar el logro de los objetivos Institucionales.

De igual forma estas acciones, documentos y procedimientos han permitido un alcance del 100% en el Plan de Tratamiento de Riesgos para el año 2024, de acuerdo a las acciones y líneas establecidas, resaltando las siguientes:

- Actualización de la Política de Seguridad y Privacidad de la Información
- Actualización de la Matriz de activos de información de la ANT
- Mapa de Riesgos de Seguridad de la Información
- Creación del procedimiento para la Administración de Riesgos de Seguridad de la Información
- Creación del Instructivo para la identificación de riesgos y verificación de controles existentes
- Creación del Manual del Sistema de Gestión de Seguridad de la Información
- Actualización de 9 documentos relacionados con Seguridad de la Información.
- Desarrollo del Plan de capacitación y socialización sobre conceptos y procedimientos de Seguridad de la Información

ACTIVIDAD	ENTREGABLE	ALCANCE 2024
Elaboración Plan de Trabajo - Revisión, ajuste y aprobación del mismo	Plan de trabajo	100%
Identificación nuevos activos de información (contrastar activos de información Publicados Vs. los identificados como infraestructura crítica)	Inventario de activos Índice de Clasificación y Reserva	100%
Actualización Matriz de Activos de Información con su respectiva valoración	Matriz de activos	100%
Articulación en mesas de trabajo para revisión de la matriz actualizada con los líderes de TI (AE, BPM, BD RESO, Aplicaciones, EIST)	Registros de asistencia mesas técnicas	100%
Elaboración del acta de aprobación de la Matriz de Activos de Información actualizada, gestionar firmas del acta	Acta de aprobación	100%
Identificación de los riesgos sobre los activos de información (SSIT, Infraestructura y soporte tecnológico, y 3 procesos misionales: Gestión de la información, Evaluación del impacto del ordenamiento social de la propiedad, Administración de tierras)	Matriz de evaluación de riesgos de seguridad de la información	100%
Valoración o Tratamiento de los riesgos de seguridad de la información: Análisis, evaluación, estrategia de mitigación, herramientas de gestión,. (Mesas de trabajo con usuarios de la SSIT, Infraestructura y soporte tecnológico, 3 procesos misionales: Gestión de la información, Evaluación del impacto del ordenamiento social de la propiedad, Administración de tierras) - Aceptación perfiles de riesgo	Matriz de riesgos Declaración de aplicabilidad	100%
Elaboración, aprobación y publicación del mapa de riesgos	Matriz de riesgos de seguridad de la información publicada	100%
Medición (verificar efectividad de los controles de seguridad) Diseñar e implementar indicadores considerando eventos de riesgos	Documento Diseño y Valoración de Controles	100%
Elaboración Informe de medición controles de seguridad	Informe Medición controles de seguridad	100%

FASE 1 - Identificación de necesidades para desarrollar herramienta para gestionar los Riesgos de Seguridad Digital Tablero de control	Herramienta diseñada	100%
FASE 2 - Desarrollar herramienta para gestionar los Riesgos de Seguridad Digital Tablero de control- Identificación de necesidades	Herramienta diseñada	100%
FASE 3 - Implementar una herramienta para gestionar los Riesgos de Seguridad Digital Tablero de control basado en los indicadores.	Herramienta implementada	100%
Generar estrategia de comunicación para la capacitación sobre seguridad digital y ciberseguridad	Seguimiento a cronograma de capacitación	100%
Actualización de la documentación sobre seguridad de la información	Documentos actualizados	100%
Cargue de la información en el repositorio	Evidencia de información en el repositorio	100%

Cabe resaltar que, si bien se había proyectado la identificación de riesgos para la Subdirección de Sistemas de información de Tierras, el Equipo de Infraestrutura y Soporte Tecnológico y 3 procesos misionales: Gestión de la información, Evaluación del impacto del ordenamiento social de la propiedad, Administración de tierras, se logró la identificación para todos los procesos y dependencias de la ANT

Ahora bien, este proceso permite que actualmente la ANT cuente con el Mapa de Riesgos de Seguridad de la Información, en el cual se han identificado 110 riesgos y se han evaluado 43 controles de los 93 que se encuentran en el anexo A de la ISO 27001, sin embargo, cabe aclarar, que se ha hecho una verificación de los 93 controles de la norma, en un proceso paralelo, lo que permite contar con la Declaración de Aplicabilidad en su totalidad.

De esta manera se establece un plan de acción que contiene 117 acciones preventivas que hacen parte integral del presente Plan para su seguimiento durante el año 2025, el cual contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos de información, estas actividades se estructuraron de la siguiente manera:

Ítem	Actividad
1	Elaboración Plan de Trabajo sobre acciones y controles evaluados en el proceso de identificación de riesgos - Revisión, ajuste y aprobación del mismo
2	Socialización por dependencias de: las matrices de riesgos, controles verificados y acciones preventivas establecidas en el proceso de identificación de riesgos.
3	Actualización del instructivo para la valoración de activos de información de acuerdo a la herramienta diseñada
4	Actualización Matriz de Activos de Información con su respectiva valoración, mediante el desarrollo de mesas técnicas
5	Publicación de Activos de Información
6	Revisión y actualización del procedimiento para administración de riesgos de seguridad de la información
7	Identificación de Riesgos de Seguridad y Privacidad de la Información
8	Establecimiento de acciones preventivas - Aceptación perfiles de riesgo

9	Ejercicios trimestrales de inspecciones a controles de acuerdo con SoA
10	Consolidación, aprobación y publicación del mapa de riesgos
11	Elaboración Informe de Riesgos de seguridad de la información y medición controles de seguridad

7. Recursos

Recursos	Variable
Humanos	La Subdirección de Sistemas de Información es responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Entidad en lo concerniente a la seguridad y privacidad de la información lo cual contribuye a la mejora continua.
Técnicos	Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 6 -DAFP 2022. Modelo Nacional de gestión de riesgos de seguridad de la información para entidades públicas MinTIC 2021. Herramienta para la gestión de riesgos (Matriz de Riesgos SGSI) Procedimiento para administración de riesgos de seguridad de la información
Logísticos	Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.
Financieros	Recursos para la adquisición de conocimiento, recursos humanos, técnicos y el desarrollo de consultorías y auditorías.

8. Presupuesto

El presupuesto para el desarrollo del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información identificados en la entidad debe ser asumido por la Dirección donde se esté atendiendo el incidente de seguridad, quien será el responsable directo de la verificación, seguimiento y atención de la implementación de los controles definidos en el plan de tratamiento.

9. Medición

El proceso de verificación del proceso se realiza bajo la valoración de los indicadores de gestión creados, medición de la eficacia y eficiencia de los controles de seguridad de la información, así como sobre el seguimiento a las acciones preventivas establecidas, este procedimiento debe realizarse de manera periódica bajo un cronograma de verificación que permita documentar la implementación, alcance, soportes y validación de los incidentes presentados y acciones implementadas. El control del proceso de medición estará a cargo de la SSIT y su equipo de Seguridad de la Información.

10. 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 Sistemas de gestión de la seguridad de la información.
- DEST–P-011 Procedimiento Administración de Riesgos de Seguridad de la Información
- Matriz de Riesgos de Seguridad de la Información de la entidad
- DEST-F-001 Mapa de Gestión de Riesgos de seguridad de la Información
- DEST-P-001 Administración de Riesgos de Gestión
- INTI-Plan-005 Plan de tratamiento de riesgos 2024 ANT
- DEST-POLÍTICA-001 Política Administración del Riesgo
- Plan tratamiento de Riesgos de seguridad y privacidad de la información versión 6 2024 – MINTIC

11. Referencias

- MinTIC, (2018). Modelo nacional de gestión de riesgos de seguridad digital (MGRSD).
- MinTIC, (2018). Guía para la gestión de riesgos de seguridad digital para el Gobierno nacional, territoriales y sector público.
- DAFP, (noviembre de 2022). Guía para la administración del riesgo y el diseño de controles en entidades públicas VERSIÓN 6.
- Lledo, P. (2017). Administración de proyectos: El ABC para un director de proyectos exitoso. Pablo Lledó.

HISTORIAL DE CAMBIOS		
Fecha	***Versión***	***Descripción***
23 de enero de 2023	1	Primera versión del documento. Se elabora este documento como parte de la implementación de la gestión de riesgos de seguridad digital para asegurar la confidencialidad, integridad y disponibilidad de los activos de información.
17 de enero de 2024	2	Segunda versión del documento. Se realiza actualización del presente documento como parte de la implementación de la gestión de riesgos de seguridad digital con el fin de asegurar la confidencialidad, integridad y disponibilidad de los activos de información de la entidad.
23 de enero de 2025	3	Tercera versión del documento. Se realiza actualización del presente documento como parte de la implementación de la gestión de riesgos de seguridad de la información con el fin de asegurar la confidencialidad, integridad y disponibilidad de los activos de información de la entidad.

Elaboró:	**Revisó:**	**Aprobó:** Comité Institucional de Gestión y Desempeño (Resolución 183 de 2018)
Rosa Johanna Rincón Molina	Diana Lucia Herrera Riaño	
Cargo: Contratista – Subdirección de Sistemas de Información de Tierras	**Cargo**: subdirectora de Sistemas de Información de Tierras	**Cargo:** Comité Institucional de Gestión y Desempeño, Sesión 1 del 23 de enero de 2025.
Firma: **ORIGINAL FIRMADO**	**Firma:** **ORIGINAL FIRMADO**	**Firma:** **ACTA FIRMADA**