PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2024

DIRECCIÓN DE GESTION DEL ORDENAMIENTO SOCIAL DE LA PROPIEDAD

SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN DE TIERRAS

Contenido

1. Introducción

Los procesos de aseguramiento 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, permiten 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 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 en caso de incidentes de seguridad.

Este plan de tratamiento de riesgos pretende fortalecer a la ANT en procesos de identificación, análisis, clasificación, tratamiento, evaluación y mitigación de los riesgos que puedan alterar el Core de operación de la entidad, permitiendo brindar una mejora continua en la prestación de servicios y demás objetivos misionales.

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.

- Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

- 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).

- Estimación del riesgo: Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo. Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

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

- Evitación del riesgo: Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

- 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.

- Integridad: Propiedad de la información relativa a su exactitud y completitud.

- 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.

- Retención del riesgo. Aceptación de la pérdida o ganancia proveniente de un riesgo particular.

- 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.

- Tolerancia al riesgo: son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.

- 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:

Implementar la gestión de riesgos de seguridad digital basada en la definición metodológica del Modelo de Gestión de Riesgos de Seguridad Digital para asegurar la confidencialidad, integridad y disponibilidad de los activos de información de la ANT e incrementar la confianza de las múltiples partes interesadas en el uso del entorno digital.

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.

- Implementar una herramienta que permita gestionar los Riesgos de Seguridad y Ciberseguridad en la Agencia Nacional de Tierras.

- 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 Plan de Tratamiento de Riesgos de la ANT proyecta desarrollar las actividades aplicables a los activos de TI, en el período comprendido entre enero y diciembre de 2024, gestionando los riesgos detectados y evaluados que se encuentren clasificados en los niveles Moderado, Grave y Crítico acorde con los lineamientos definidos por la Entidad, los riesgos que se encuentren en nivel Bajo serán asumidos o transferidos según la necesidad.

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.

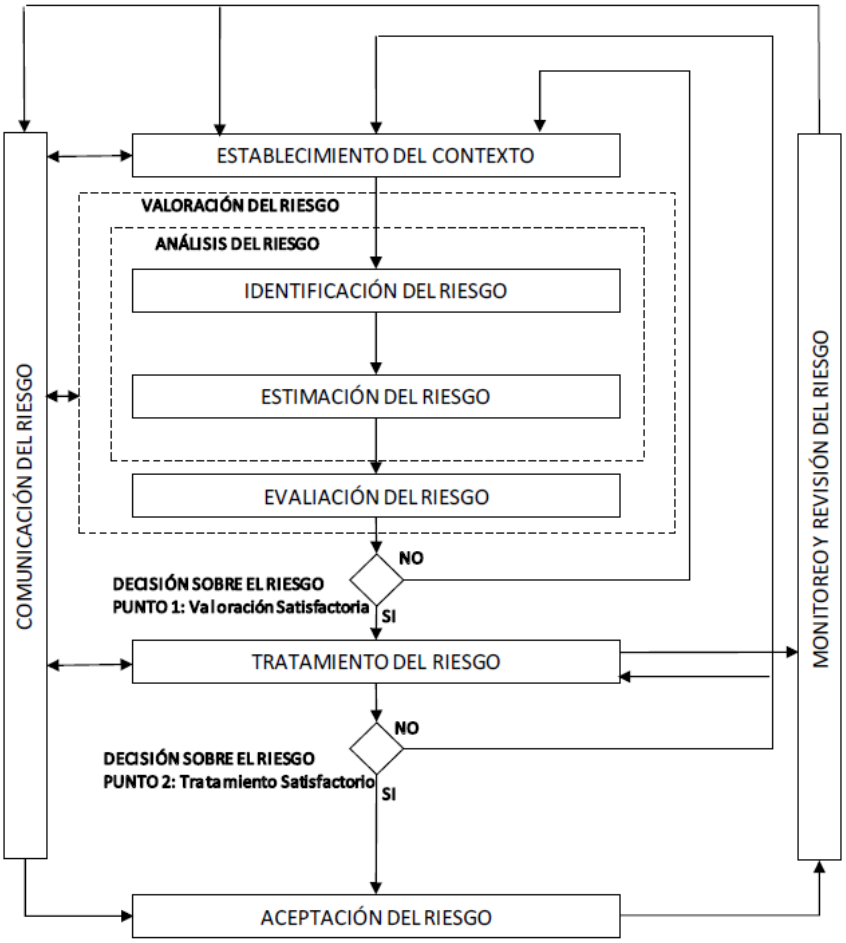
5.3. Política de seguridad de la información

Esta política propone implementar el Sistema de Seguridad de la Información – SGSI, gestionar adecuadamente los riesgos de seguridad, el cumplimiento de las obligaciones legales y contractuales vigentes y aplicables, y la mejora continua del SGSI, además de, satisfacer las necesidades y expectativas de sus partes interesadas en materia de seguridad de la información

5.4. 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.

Proceso para la administración de riesgo de seguridad de la información



Fuente: NTC-ISO IEC/27005

5.5. 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 desarrollo metodológico se plantea conforme las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información de MinTIC versión 2016, con el fin de viabilizar la ejecución del Plan de Tratamiento de Riesgos, se plantea el desarrollo por fases, las cuales cubre uno o varios

activos de TI (información, sistemas de información, bases de datos, infraestructura y servicios de TI) de acuerdo al nivel de complejidad y criticidad que representa para la Agencia.

La descripción de las fases y los activos es el siguiente:

- FASE 1: Sistema de Información de Tierras – SIT (Subsistemas: SIDRA, Galería de reportes, Gestión FNA, etc.,) y Orfeo.
- FASE 2: Barrido Predial Masivo – BPM, BD Procesos Agrarios y SIG Formalización.
- FASE 3: RESO, SART, Bodega de datos (SharePoint), SINERGIA y otros sistemas de información críticos.

Plan de tratamiento de riesgos de seguridad Digital		
	Actividad	Responsable
	Planeación	
1	Elaboración Plan de Trabajo	SSIT
2	Revisión, ajustes y aprobación Plan de Trabajo	SSIT
	Ejecución	
3	Identificación nuevos activos de información (contrastar activos de inf. Publicados Vs. los identificados como infraestructura crítica)	SSIT
4	Actualización Matriz de Activos de Información con su respectiva valoración	SSIT
5	Articulación en mesas de trabajo para revisión de la matriz actualizada con los líderes de TI (AE, BPM, BD RESO, Aplicaciones, EIST)	SSIT
6	Elaboración del acta de aprobación de la Matriz de Activos de Información actualizada, gestionar firmas del acta	SSIT, EIST
7	Gestionar aprobación ante el Comité institucional de Gestión y Desempeño	SSIT
8	Gestionar publicación de Matriz de Activos de información actualizada 2024 en la página web de la ANT.	SSIT
	FASE 1 - SIT y Orfeo	
9	Identificación de los riesgos sobre los nuevos activos de información (puntos de riesgo, impacto, factores, clasificación del riesgo. (Mesas de trabajo con usuarios del área misional, EIST, responsable aplicación, responsable de la información)	SSIT, EIST, otros
10	Valoración o Tratamiento de los riesgos de seguridad digital: Análisis, evaluación, estrategia de mitigación, herramientas de gestión, monitoreo y revisión. (Mesas de trabajo con usuarios del área misional, EIST, responsable aplicación, responsable de la información)	SSIT, EIST
11	Elaboración de controles asociados (Anexo A ISO/IEC 27001:2013)	SSIT
12	Identificación de necesidades para desarrollar herramienta para gestionar los Riesgos de Seguridad Digital Tablero de control	SSIT
	FASE 2 - BPM, BD Procesos Agrarios y SIG Formalización	
13	Identificación de los riesgos sobre los nuevos activos de información (puntos de riesgo, impacto, factores, clasificación del riesgo)	SSIT, EIST
14	Valoración o Tratamiento de los riesgos de seguridad digital: Análisis, evaluación, estrategia de mitigación, herramientas de gestión, monitoreo y revisión.	SSIT, EIST
15	Elaboración de controles asociados (Anexo A ISO/IEC 27001:2013)	SSIT
16	Desarrollar herramienta para gestionar los Riesgos de Seguridad Digital Tablero de control- Identificación de necesidades.	SSIT
	FASE 3 - RESO, SART, Bodega Datos (Sharepoint), Sinergia y otros SI	
17	Identificación de los riesgos sobre los nuevos activos de información (puntos de riesgo, impacto, factores, clasificación del riesgo)	SSIT, EIST

18	Valoración o Tratamiento de los riesgos de seguridad digital: Análisis, evaluación, estrategia de mitigación, herramientas de gestión, monitoreo y revisión.	SSIT, EIST
19	Elaboración de controles asociados (Anexo A ISO/IEC 27001:2013)	SSIT
20	Generación de mapa de riesgos	SSIT
21	Elaboración de memorando y aprobación del mapa de riesgos	SSIT
22	Generar estrategia de comunicación para la capacitación sobre seguridad digital y ciberseguridad	SSIT
23	Actualización de la documentación sobre seguridad de la información	SSIT
24	Medición (verificar efectividad de los controles de seguridad) Diseñar e implementar indicadores considerando eventos de riesgos	SSIT
25	Elaboración Informe de medición controles de seguridad	SSIT
26	Implementar una herramienta para gestionar los Riesgos de Seguridad Digital Tablero de control basado en los indicadores.	SSIT
27	Cargue de la información en el repositorio	SSIT

Los controles seleccionados serán cruzados con los estándares ISO 27001:2013 y su anexo A, que permite determinar las vulnerabilidades.

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)
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, este procedimiento debe realizarse de manera periódica bajo un cronograma de auditoría que permita documentar la implementación, alcance, soportes y validación de los incidentes presentados. El control del proceso de medición estará a cargo de la SSIT y sus equipos.

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 27001:2013 Sistemas de gestión de la seguridad de la información.
- Matriz de Riesgos de Seguridad de la Información
- DEST-F-001 Mapa de Gestión de Riesgos
- DEST-P-001 Administración de Riesgos de Gestión
- INTI-Plan-005 Plan de tratamiento de riesgos 2022 ANT
- DEST-POLÍTICA-001 Política Administración del Riesgo
- Plan tratamiento de Riesgos de seguridad y privacidad de la información versión 5 2023 – 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, (diciembre de 2020). Guía para la administración del riesgo y el diseño de controles en entidades públicas VERSIÓN 5.

- MinTIC, (2018). Guía para la gestión de riesgos de seguridad digital para el Gobierno nacional, territoriales y sector público.

- 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.

Elaboró:	**Revisó:**	**Aprobó:** Comité Institucional de Gestión y Desempeño (Resolución 183 de 2018)
Andrea Linney Sierra Ladino	Diana Lucia Herrera Riaño	
Cargo: Contratista – Secretaría General	**Cargo**: Subdirectora Sistemas de Información de Tierras	**Cargo**: Comité Institucional de Gestión y Desempeño, Sesión 1 del 17 de enero de 2024
Firma: **ORIGINAL FIRMADO**	**Firma:** **ORIGINAL FIRMADO**	**Firma:** **ACTA FIRMADA**