PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2026

DIRECCIÓN DE GESTIÓN DEL ORDENAMIENTO SOCIAL DE LA PROPIEDAD

SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN DE TIERRAS

Contenido

1. Introducción 3
2. Términos y definiciones 3
3. Objetivos 6
   3.1. Objetivo General 6
   3.2. Objetivos Específicos 7
4. Alcance 7
5. Marco de referencia 7
   5.1. Política de administración del Riesgo 7
   5.2. Procedimiento de administración de riesgos de gestión 7
   5.3. Política General de seguridad y privacidad de la información 8
   5.4. Procedimiento para la Administración de riesgos de seguridad de la información 8
   5.5. Guía de gestión de riegos 8
6. Metodología 8
7. Recursos 10
8. Presupuesto 10
9. Medición 10
   1. *Enfoque de medición* 11
   2. *Indicadores de medición* 11
   3. *Frecuencia y responsables* 12
   4. *Mecanismos de seguimiento y reporte* 12
   5. Uso de los resultados 12
10. Documentos Asociados 12

1. Introducción

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Agencia Nacional de Tierras (ANT) se fundamenta en una orientación estratégica que promueve el fortalecimiento de una cultura organizacional de carácter preventivo. En este sentido, la adecuada comprensión del concepto de riesgo, junto con el análisis del contexto interno y externo de los procesos institucionales, permite la formulación de acciones orientadas a reducir los impactos negativos que podrían generarse ante la materialización de eventos de riesgo, salvaguardando así la continuidad y el cumplimiento de la misión institucional.

De manera complementaria, el presente Plan busca establecer y consolidar estrategias sistemáticas para la identificación, análisis, evaluación, tratamiento y monitoreo de los riesgos de seguridad y privacidad de la información, bajo criterios de objetividad y mejora continua. Lo anterior con el propósito de visibilizar aquellas situaciones que puedan comprometer el logro de los objetivos estratégicos asociados al Entorno TIC para el Desarrollo Digital, ciudadanos y hogares empoderados en el entorno digital, la Transformación Digital Sectorial y Territorial, así como la Inclusión Social Digital.

Este enfoque se desarrolla en concordancia con las disposiciones del Documento CONPES 3995 de 2020 y el Decreto Único Reglamentario del Sector TIC – Decreto 1078 de 2015, el cual define el habilitador de seguridad y privacidad de la información, reglamentado mediante la Resolución 500 de 2021. En este marco, la ANT adopta los lineamientos y estándares del Modelo de Seguridad y Privacidad de la Información (MSPI), incorporando las buenas prácticas de los estándares internacionales ISO/IEC 27001:2022 e ISO 31000:2018, así como la Guía para la administración del riesgo y el diseño de controles en entidades públicas establecida en el Modelo Integrado de Planeación y Gestión (MIPG).

En atención a lo anterior, el presente documento se actualiza dando cumplimiento a lo establecido en el Decreto 612 de 2018, con el fin de fortalecer y mantener vigente el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información en la Agencia Nacional de Tierras.

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

Gestionar de manera integral y eficiente los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios en la Agencia Nacional de Tierras (ANT), mediante la definición e implementación de acciones de tratamiento que permitan prevenir, reducir o mitigar eventos o incidentes que puedan afectar el cumplimiento de los objetivos institucionales y la toma de decisiones informadas.

3.2. Objetivos Específicos

1. Establecer los lineamientos institucionales para la identificación, análisis, evaluación, tratamiento y monitoreo de los riesgos de Seguridad y Privacidad de la Información en la Agencia Nacional de Tierras, en concordancia con el Modelo de Seguridad y Privacidad de la Información (MSPI) y el MIPG.
2. Definir planes de acción para los riesgos clasificados en niveles Moderado, Alto y Extremo, orientados al fortalecimiento y mejora de los controles existentes, conforme a los lineamientos y buenas prácticas establecidos.
3. Garantizar la integración de la gestión de riesgos de seguridad de la información y continuidad de la operación en los procesos institucionales, contribuyendo a la prevención de incidentes que puedan afectar la disponibilidad, confidencialidad e integridad de la información.
4. Asegurar el seguimiento y monitoreo permanente de los riesgos aceptados en niveles Bajo o Aceptable, mediante la ejecución de los controles definidos en los mapas de riesgos de los procesos y su articulación con el Plan Operativo del Sistema de Gestión de Seguridad y Privacidad de la Información.
5. Fortalecer la cultura de gestión del riesgo y la toma de decisiones basada en riesgos al interior de la Entidad, promoviendo la adopción de buenas prácticas en Seguridad y Privacidad de la Información y Seguridad Digital.
6. 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 aplica a la gestión de la mitigación de riesgos identificados en el año 2025 y se desarrollará entre enero y diciembre de 2026, teniendo en cuenta que se han establecido acciones preventivas para aquellos riesgos residuales con niveles extremos, altos o moderados.

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 General 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 la Administración 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 para la Gestión Integral de Riesgos versión 7 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.

6. Metodología

El Departamento Administrativo de la Función Pública (DAFP) actualizó en agosto de 2025 la Guía para la Administración Integral del Riesgo en Entidades Públicas, con el propósito de unificar y fortalecer la metodología para la gestión efectiva de los riesgos de corrupción, gestión, fiscales y de seguridad digital en las entidades del Estado. Dicha guía incorpora criterios para la evaluación objetiva de la efectividad de los controles implementados, así como la adopción del esquema de Líneas de Defensa, mediante el cual se definen roles, responsabilidades y niveles de aseguramiento en la gestión del riesgo, en concordancia con los principios del Modelo Integrado de Planeación y Gestión (MIPG).

En concordancia con este marco normativo y metodológico, y en alineación con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y el estándar ISO/IEC 27001:2022, la Agencia Nacional de Tierras (ANT) actualiza de manera periódica su Política de Seguridad y Privacidad de la Información, así como el Procedimiento para la Administración de Riesgos de Seguridad de la Información. Estos instrumentos establecen los lineamientos institucionales para la identificación, análisis, evaluación, tratamiento, monitoreo, revisión y seguimiento de los riesgos de seguridad de la información, bajo un enfoque preventivo que permita anticipar su materialización y minimizar los impactos que puedan afectar el cumplimiento de los objetivos institucionales.

Como resultado de la aplicación de esta metodología, la ANT ha identificado un total de noventa (90) riesgos de seguridad de la información y ha evaluado cincuenta (50) controles de los noventa y tres (93) establecidos en el Anexo A de la norma ISO/IEC 27001:2022. Este ejercicio permitió definir sesenta y dos (62) acciones preventivas, las cuales hacen parte integral del presente Plan de Tratamiento de Riesgos. Dichas acciones contemplan la definición de actividades orientadas a mitigar los riesgos asociados a los activos de información de la Entidad, las cuales se estructuran de la siguiente manera:

Plan de Tratamiento de Riesgos de Seguridad de la Información				
Ítem	**Actividad**	**Responsable**	**FECHA INICIO**	**FECHA FIN**
1	Elaboración Plan de Trabajo sobre acciones y controles evaluados en el proceso de identificación de riesgos - Revisión, ajuste y aprobación del mismo	SSIT	1/02/2026	28/02/2026
2	Socialización por dependencias: matrices de riesgos, controles verificados y acciones preventivas establecidas en el proceso de identificación de riesgos.	SSIT	16/02/2026	28/05/2026
3	Seguimiento a implementación de acciones preventivas y controles establecidos	SSIT	10/03/2026	15/12/2026
4	Revisión y actualización si aplica, del procedimiento y el instructivo del instructivo para la valoración de activos de información.	SSIT	16/02/2026	31/03/2026
5	Actualización Matriz de Activos de Información con su respectiva valoración, mediante el desarrollo de mesas técnicas	SSIT	1/04/2026	30/06/2026
6	Revisión y aprobación de la matriz de activos de información de la entidad	SSIT - EIST	01/10/2026	30/10/2025
7	Publicación del INTI-F-020 REGISTRO ACTIVOS DE INFORMACIÓN y el INTI-F-022 INFORMACIÓN CLASIFICADA Y RESERVADA	SSIT	01/10/2026	30/10/2025
8	Revisión y actualización si aplica, del procedimiento para administración de riesgos de seguridad de la información	SSIT	10/03/2026	31/05/2026
9	Identificación y valoración de riesgos sobre los activos de información en la entidad (vigencia 2026)	SSIT	1/07/2026	30/11/2026

Plan de Tratamiento de Riesgos de Seguridad de la Información				
Ítem	**Actividad**	**Responsable**	**FECHA INICIO**	**FECHA FIN**
10	Establecimiento de acciones preventivas vigencia 2027 - Aceptación perfiles de riesgo	SSIT	1/07/2026	30/11/2026
11	Medición y verificación de los controles de seguridad de acuerdo al proceso de identificación de riesgos de seguridad de la información	SSIT	1/07/2026	30/11/2026
12	Consolidación y aprobación para publicación del mapa de riesgos	SSIT	1/10/2026	31/12/2026
13	Elaboración Informe de Riesgos de seguridad de la información y medición controles de seguridad	SSIT	1/11/2025	30/11/2026

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 gestión integral del riesgo en entidades públicas Versión 7 -DAFP 2025. 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 Política General de Seguridad y Privacidad de la Información Política de Protección de datos personales
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 Plan de Tratamiento de riesgos tiene una verificación mensual, mediante el cual se hace seguimiento a las acciones e indicadores establecidos.

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 proceso se realiza trimestralmente bajo un cronograma de verificación que permita documentar la implementación, alcance, soportes y validación de las acciones implementadas. El control del proceso de medición estará a cargo de la SSIT y su equipo de Seguridad de la Información.

Esta estrategia de medición del Plan de Tratamiento de Riesgos de Seguridad de la Información de la Agencia Nacional de Tierras (ANT) se fundamenta en un enfoque basado en riesgos y en la mejora continua, conforme a lo establecido en la norma ISO/IEC 27001:2022 (cláusulas 6.1, 9.1 y 10), los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y el esquema de seguimiento y evaluación del Modelo Integrado de Planeación y Gestión (MIPG).

Esta estrategia tiene como propósito evaluar de manera periódica el avance, la efectividad y el impacto de las acciones preventivas definidas en el Plan, así como la eficiencia de los controles implementados para el tratamiento de los riesgos de seguridad y privacidad de la información.

1. *Enfoque de medición*

La medición se realizará a partir de tres dimensiones principales:

- **Cumplimiento del Plan de Tratamiento**: seguimiento al grado de ejecución de las acciones preventivas definidas.
- **Efectividad de los controles**: evaluación del desempeño de los controles implementados para mitigar los riesgos identificados.
- **Nivel de riesgo residual**: verificación de la reducción del nivel de riesgo posterior a la implementación de las acciones de tratamiento.

2. *Indicadores de medición*

Para garantizar una evaluación objetiva, se establecerán indicadores alineados con los objetivos del Plan, tales como:

- **Porcentaje de acciones del Plan de Tratamiento ejecutadas**
  (Acciones ejecutadas / Acciones programadas) × 100
- **Porcentaje de controles evaluados como efectivos**
  (Controles efectivos / Controles evaluados) × 100
- **Variación del nivel de riesgo residual**
  Comparación entre el nivel de riesgo inherente y el nivel de riesgo residual posterior al tratamiento.
- **Número de riesgos en niveles Alto y Extremo**
  Medición periódica del comportamiento de los riesgos críticos antes y después de la implementación del Plan.
- **Porcentaje de riesgos con seguimiento vigente**
  (Riesgos monitoreados / Total de riesgos identificados) × 100

3. *Frecuencia y responsables*

- La medición se realizará de manera **trimestral**, sin perjuicio de seguimientos extraordinarios cuando se presenten incidentes de seguridad de la información o cambios significativos en el contexto del riesgo.
- Los **líderes de proceso** serán responsables de reportar el avance de las acciones asignadas.
- La **Segunda Línea de Defensa**, a través del responsable del Sistema de Gestión de Seguridad y Privacidad de la Información, consolidará y analizará los resultados.
- La **Tercera Línea de Defensa** realizará verificaciones independientes en el marco de auditorías internas o evaluaciones de control.

4. *Mecanismos de seguimiento y reporte*

Los resultados de la medición serán documentados y reportados a través de:

- Informes periódicos de seguimiento del Plan de Tratamiento de Riesgos.
- Tableros de control según lo establecido por la Oficina de Planeación.
- Reportes al Comité Institucional de Gestión y Desempeño o a la instancia que haga sus veces.
- Insumos para la Revisión por la Dirección, conforme a la cláusula 9.3 de ISO/IEC 27001:2022.

5. Uso de los resultados

Los resultados de la medición permitirán:

- Identificar desviaciones, debilidades o controles inefectivos.
- Definir acciones correctivas o de mejora.
- Actualizar el nivel de riesgo residual y priorizar nuevas acciones de tratamiento.
- Fortalecer la toma de decisiones basada en riesgos y el cumplimiento de los objetivos institucionales.

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 2025 ANT
- DEST-POLÍTICA-001 Política Administración del Riesgo

HISTORIAL DE CAMBIOS		
Versión	**Descripción**	**Fecha**
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.	23/01/2023
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.	17/01/2024
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.	23/01/2025
4	Cuarta versión del documento. Se realiza actualización del presente documento de acuerdo al decreto 612 de 2018 y 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.	27/01/2026

APROBACIÓN				
	NOMBRE	**CARGO**	**FIRMA**	**FECHA**
ELABORÓ	Rosa Johanna Rincón Molina	Contratista - Subdirección Sistema Información de Tierras	**ORIGINAL FIRMADO**	21/01/2026
REVISÓ	Diana Lucía Herrera Riaño	Subdirectora de Sistemas de Información de Tierras	**ORIGINAL FIRMADO**	23/01/2026
APROBÓ	**APROBACIÓN Y PUBLICACIÓN DE LA POLÍTICA** **1er Sesión Comité Institucional de Gestión y Desempeño del 27/01/2026**			