OBJETIVO	Determinar 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
ALCANCE	Inicia desde la comprensión del contexto de la ANT como base para la identificación de los Riesgos de seguridad de la información, continua con la identificación y valoración del riesgo hasta la evaluación de la efectividad del tratamiento de riesgo establecido.
RESPONSABLE	Subdirección de sistemas de información de tierras

1. DEFINICIONES

Acciones: Mecanismos o estrategias a llevar a cabo para evitar, reducir, asumir o compartir el riesgo.

Activos de información: Según la norma ISO 27001, un activo de información es todo aquello que tiene algún valor para la organización y que, por ende, debe protegerse. Este activo contiene información, ya sea en medios digitales, en papel o en otros medios y pueden ser tangibles o intangibles.

Amenaza: Es una acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información.

Análisis de Riesgos: Establecimiento de la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar.

Causas: Medios, circunstancias, factores o agentes que pueden generar la materialización el riesgo.

Calificación del riesgo: Se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo.

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados

Contexto de la organización: Cuestiones internas y externas de la Agencia Nacional de Tierras, tanto de carácter social, económico, cultural, de orden público, político, legal y cambios tecnológicos, entre otros.

Consecuencias: Efectos o situaciones resultantes de la materialización del riesgo que impactan, en alguna medida, en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Control: Mecanismos o estrategias establecidas para disminuir la probabilidad de ocurrencia del riesgo, el impacto de los riesgos y/o asegurar la continuidad del servicio en caso de llegarse a materializar el riesgo.

Control automático: son ejecutados por un sistema.

Control correctivo: control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

Control detectivo: control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.

Control manual: controles que son ejecutados por personas.

Control preventivo: control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.

Descripción: Se refiere a las características generales o las formas en que se observa o manifiesta el riesgo identificado.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

Evaluación: Nivel en que se encuentra el riesgo resultado de calificar el riesgo con base a la probabilidad y el impacto de ellos.

Evento: Ocurrencia o cambio de un conjunto particular de circunstancias (Evento= es un riesgo materializado).

Impacto: Consecuencias pueden afectar al proceso o a la entidad si se llega a materializar el riesgo.

Integridad: Propiedad de exactitud y completitud.

Mapa de riesgos: documento con la información resultante de la administración del riesgo.

Política para la gestión de riesgos y oportunidades: Declaración de la Dirección general de sus intenciones globales con respecto a los Riesgos y Oportunidades.

Probabilidad: Posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de "frecuencia", cuando existen datos verificables de la previa materialización del riesgo en la entidad o con criterios de "factibilidad", cuando se presume que nunca antes se ha materializado el riesgo en la entidad.

Plan de Acciones Preventivas: Conjunto de acciones preventivas dirigidas al fortalecimiento de los controles para la mitigación del riesgo, donde se define la acción, tiempo de ejecución, evidencia y responsable.

Responsables: Dependencias o funcionarios encargados de asegurar la ejecución de las acciones para el tratamiento de los Riesgos.

Riesgos: Efecto de la incertidumbre sobre los objetivos de la Agencia Nacional de Tierras.

Riesgo de Gestión: Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

Riesgos Estratégicos: Afectan el cumplimiento de los objetivos del Plan Estratégico de la Agencia Nacional de Tierras.

Riesgos Inherente: Riesgo permanente que no se puede separar de una actividad o de un proceso, por formar parte de su naturaleza. Se considera riesgo inherente el que es evaluado sin reconocer y sin valorar el efecto de los controles que ya están establecidos en los procesos y procedimientos de la entidad.

Riesgos Residual: Nivel de riesgo que permanece luego de reconocer y valorar el efecto que los controles, ya establecidos en la entidad, tienen sobre el nivel de riesgo inherente.

Riesgo de Seguridad de la Información: 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)

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.

Valoración: Resultado de confrontar el riesgo con la calidad de los controles existentes.

Vulnerabilidad: Se trata de una debilidad o fallo en un sistema de información que abre la puerta para que un atacante o situación no prevista pueda comprometer la integridad, disponibilidad o confidencialidad de los datos.

2. GENERALIDADES

De acuerdo a las generalidades establecidas por la Agencia Nacional de Tierras en la Política de Administración de Riesgos DEST-POLITICA-001, así como la INTI-Política-001 Política General de Seguridad y Privacidad de la Información, una organización inteligente y proactiva planifica y toma decisiones con un pensamiento basado en riesgos, que le permite anticiparse a los problemas y alcanzar óptimos niveles de eficacia, alcanzar cada vez mejores resultados, prevenir los efectos negativos de las dinámicas del contexto y promover las situaciones favorables que la impulsen a alcanzar los resultados previstos.

En relación a seguridad de la información se deben tener claridad en los tres pilares que fundamentan este concepto:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

2.1. Contexto Interno

La Dirección General de la Agencia Nacional de Tierras se ha propuesto que la planeación de procesos y planes se fundamente en la administración de los riesgos, implementando metodologías que fueron la base para la elaboración de este procedimiento, propuestas por el Departamento Administrativo de la Función Pública y por los organismos internacionales expertos: Organización Internacional de Estandarización - ISO y Comité de Organizaciones Patrocinadoras de la Comisión Treadway - COSO, por sus siglas en ingles.

Este procedimiento orienta a las dependencias de la entidad en la identificación, análisis y valoración de los riesgos de seguridad de la información que pueden afectar el desempeño de los procesos y planes, y orienta también en el establecimiento y aplicación de controles que funcionan antes de emprender las tareas operativas cotidianas, mientras las tareas suceden o, incluso, después de finalizadas.

Los controles son mecanismos o estrategias establecidas para disminuir la probabilidad de ocurrencia y el impacto de los riesgos, además de asegurar la continuidad del servicio en caso de llegarse a materializar el riesgo. Los principales controles que, en la Agencia Nacional de Tierras, son tareas cotidianas preventivas, detectivas o

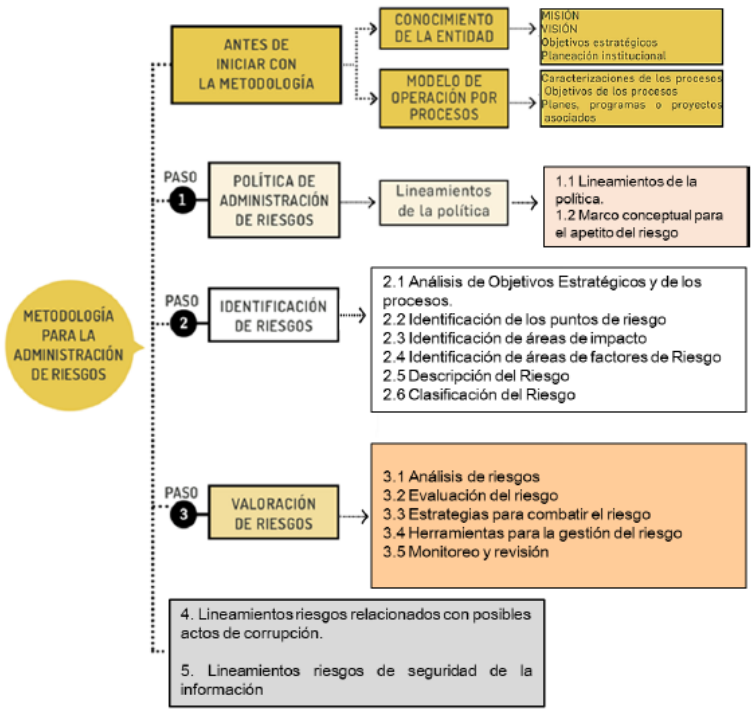
correctivas establecidas en políticas, procedimientos e incluso algunas buenas prácticas que no están documentadas, pero que contribuyen a garantizar que se mitiguen los riesgos en toda la entidad, en todos los niveles y en todas las funciones; por lo tanto, es necesario que todo el personal de la ANT conozca cuáles son las tareas de control que debe ejecutar.

Para facilitar la identificación de las tareas críticas y de las correspondientes tareas de control, los procedimientos documentados de la ANT presentan el siguiente método de señalización:

Tareas Críticas	Son las tareas donde se puede materializar un riesgo que impacte negativamente el logro del objetivo del procedimiento. En la matriz de desarrollo del procedimiento y en el diagrama de flujo se identifican tareas críticas con texto en color rojo y con el símbolo Ⓡ
Tareas de Control	Son las tareas que permiten prevenir o corregir el impacto de los riesgos en el logro del objetivo del procedimiento. En la matriz de desarrollo del procedimiento y en el diagrama de flujo se identifican tareas de control con texto en color azul y con el símbolo Ⓒ

La Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, permite establecer una estructura general para la administración y tratamiento de los riegos en las entidades públicas, la cual está en concordancia con el componente de Administración del Riesgo establecido en el Manual Estándar de control Interno para el Estado Colombiano en la Identificación, Valoración, análisis y Seguimiento y Monitoreo de los mismo en una entidad.

Metodología para la administración del riesgo



Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2022.

Como se observa y como lo estable la NTC 27005 el proceso de gestión de riesgos para la seguridad de la información puede ser iterativo para las actividades de evaluación y/o tratamiento del riesgo, aspecto que permitirá un mayor detalle de estudio y un mejoramiento de los controles para el riesgo.

De esta forma el modelo presenta un procedimiento que se realiza en las siguientes etapas:

COMUNICACIÓN Y CONSULTA: En esta etapa se busca establecer acciones que promuevan la concientización en cada una de las de las dependencias en relación a la comprensión del riesgo, lo que permite obtener una retroalimentación que conlleve al reconocimiento y tratamiento de riesgos, así como a la aplicación de controles para una mejor toma de decisiones.

ALCANCE, CONTEXTO Y CRITERIOS: Esta etapa tiene como objetivo asegurar que la evaluación del riesgo sea eficaz y que el tratamiento del mismo sea el más apropiado en relación a las necesidades y requerimientos de la ANT, de esta forma se establece el alcance, lo que implica definir cada uno de los procesos, planes, dependencias, entre otros sobre las cuales se hará la identificación, valoración y tratamiento de los riesgos de seguridad de la información. En esta misma etapa se debe hacer un reconocimiento del contexto, estableciendo aquellos factores tanto externos como internos y por procesos, que pueden afectar el tratamiento de los riegos. Finalmente se deben establecer los criterios para el manejo de los riesgos y como esto apoya la toma de decisiones en la agencia, así mismo los criterios de aceptabilidad y la metodología con la cual se van a definir las valoraciones de los riesgos.

IDENTIFICACIÓN DEL RIESGO: El objetivo de esta etapa implica el desarrollo de mesas técnicas y establecimiento de procedimientos de comunicación y consulta, mediante los cuales se pueda obtener la información correspondiente para encontrar, reconocer y describir los riesgos que pueden afectar el cumplimiento de objetivos, para ello se requiere del trabajo articulado con cada una de las dependencias responsables de los procesos quienes tiene la información pertinente y actualizada acerca de las acciones que se desarrollan, el cómo se desarrollan, las posibles amenazas relacionadas con la seguridad de la información y que tan vulnerables se encuentran los procesos frente a estas, así mismo, la naturaleza de los activos y las consecuencias e impacto que puede generar la materialización de algún riesgo.

ANÁLISIS DEL RIESGO: Su propósito es comprender la naturaleza del riesgo y sus características incluyendo, cuando sea apropiado, el nivel del riesgo. El análisis del riesgo implica una consideración detallada de incertidumbres, fuentes de riesgo, consecuencias, probabilidades, eventos, escenarios, controles y su eficacia. Un evento puede tener múltiples causas y consecuencias y puede afectar a múltiples objetivos. De esta forma esta etapa implica el establecimiento de una metodología que permita durante el proceso y en primera instancia, tener una visión sobre cómo se deberán tratar los riesgos y la forma más adecuada para esto.

EVALUACIÓN DEL RIESGO: es la parte global del procedimiento que abarca la identificación del riesgo, el análisis del riesgo y la valoración del riesgo. La evaluación del riesgo se debería llevar a cabo de manera sistemática, iterativa y colaborativa, basándose en el conocimiento y los puntos de vista de las dependencias de la ANT involucradas. (NTC-ISO 31000: 2018)

VALORACIÓN DEL RIESGO: Su propósito es apoyar a la toma de decisiones e implica comparar los resultados del análisis del riesgo con los criterios del riesgo establecidos para determinar cuándo se requiere una acción adicional. Esto puede conducir a decisiones como: no hacer nada más, considerar opciones para el tratamiento del riesgo, realizar un análisis adicional para comprender mejor el riesgo, mantener los controles existentes o incluso, reconsiderar los objetivos. (NTC-ISO 31000: 2018).

TRATAMIENTO DEL RIESGO: su propósito es seleccionar e implementar opciones para abordar el riesgo e implica un método iterativo de: formular y seleccionar opciones para el tratamiento del riesgo, planificar e implementar el tratamiento del riesgo, evaluar la eficacia de ese tratamiento, decidir si el riesgo residual es aceptable y si no es aceptable, efectuar el tratamiento adicional. (NTC-ISO 31000: 2018).

SEGUIMIENTO Y REVISIÓN: Esta etapa permite mediante el seguimiento, establecer acciones de mejora continua que permitan fortalecer y asegurar la calidad de los procesos que se establecen para la administración y el tratamiento de los riesgos de seguridad de la información, de igual permitirá una retroalimentación continua que conlleve a la identificación y valoración de riesgos de forma iterativa permitiendo un mayor seguimiento y una mejor aplicabilidad de controles.

REGISTRO E INFORME: Sus propósitos son documentar e informar los resultados de la administración del riesgo de seguridad de la información por medio de los mecanismos más apropiados en toda la ANT, proporcionando información para la toma de decisiones.

2.2. Análisis de los objetivos de la entidad y los objetivos de los procesos

Es preciso revisar el contexto general de la entidad contemplando sus procesos y planeación institucional para conocer y entender la entidad y su entorno y determinar el análisis de riesgos y la aplicación de la metodología en general.

Por lo anterior y para adelantar una correcta administración de riesgos de seguridad de la información en la Agencia, debe realizarse el análisis e interpretación de los objetivos estratégicos de la entidad y los objetivos estratégicos de sus procesos.

Lo anterior es importante, toda vez que únicamente se deben identificar y gestionar los riesgos que impacten el logro de estos objetivos; todo riesgo que no cumpla con esta condición, no se debe considerar dentro de la administración de riesgos de seguridad de la información. A excepción de los riesgos asociados a la protección de la información personal del titular, que no necesariamente están involucrados con los objetivos estratégicos de la entidad.

Así mismo, la administración de riesgos de seguridad de la información la cual incluye los riesgos de protección de datos personales y ciberseguridad se sincroniza con los objetivos declarados en la política de seguridad y privacidad de la información de la Agencia, estableciendo los lineamientos, las actividades, los seguimientos y la mejora continua requeridos para apoyar su logro.

2.3. Asignación de Roles Y Responsabilidades en la Administración de Riesgos bajo el Esquema de Líneas de Defensa

El modelo integrado de planeación y gestión (MIPG) define la creación en todas las entidades del Comité Institucional de Gestión y Desempeño, regulado por el Decreto 1499 de 2017 y el Comité Institucional de Coordinación de Control Interno, reglamentado a través del artículo 13 de la Ley 87 de 1993 y el Decreto 648 de 2017.[1]

[1] Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6 Nov. 2022 Pág. 20 https://www.funcionpublica.gov.co/documents/28587410/34299967/Guia_administracion_riesgos_capitulo_riesgo_fiscal.pdf

En la ANT, la interacción de las dependencias en la Administración de Riesgos se ha coordinado mediante la asignación de roles específicos, de manera que no existan brechas en la cobertura de los controles ni duplicación innecesaria de tareas de monitoreo, evaluación y revisión. La asignación de roles específicos se basa en el esquema de Líneas de Defensa presentado por el Modelo Integrado de Planeación y Gestión -MIPG, en la dimensión 7 “Control interno” que desarrolla la responsabilidad de la administración del riesgo y su control a través de una línea estratégica y tres líneas de defensa.

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
Estratégica	Dirección General. Comité Institucional de Coordinación de Control Interno a cargo de la oficina de Control interno	• Establecer y aprobar la Política de Administración del Riesgo la cual incluye los niveles de responsabilidad y autoridad. • Decidir sobre las acciones que correspondan para evitar consecuencias graves para la entidad cuando se detecten incumplimientos, retrasos o actuaciones irregulares, en los controles definidos. • Definir y hacer seguimiento a los niveles de aceptación, en el Comité Institucional de Coordinación de Control Interno. • Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles. • Realimentar al Comité Institucional de Gestión y Desempeño sobre los ajustes que se deban hacer frente a la gestión del riesgo.
	Comité Institucional de Gestión y Desempeño – CIGD, a cargo de la oficina de planeación.	• Realizar seguimiento a la gestión de los riesgos institucionales, corrupción y seguridad de la información y proponer mejoras a su estructura.
Primera Línea	Subdirección de Sistemas de Información. Responsables de los Procesos Facilitadores para el SIG en los procesos	• Identificar y valorar los riesgos que pueden afectar el proceso, los programas, proyectos, planes y procedimientos a su cargo y actualizarlo cuando se requiera. • Definir y aplicar a los controles para mitigar los riesgos identificados alineados con las metas y objetivos de la entidad y proponer mejoras a la gestión del riesgo en su proceso. • Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar. • Informar a la Oficina Asesora de Planeación o quien haga sus veces (segunda línea de defensa) sobre los **riesgos materializados en los procesos, programas**, proyectos y planes a su cargo. • Reportar al Comité Institucional de Gestión y Desempeño, los avances y evidencias de la gestión de los riesgos a cargo del proceso asociado (cuando se requiera).

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
		• Presentar las acciones correctivas, preventivas y de mejora, cuando **se materializa los riesgos.**
Segunda Línea	Oficina de Planeación	• Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo.
	Administrador del SGSI a cargo de la Subdirección de sistemas de información.	• Presentar ante el Comité de Gestión y Desempeño Institucional, la gestión adelantada de los riesgos en la respectiva vigencia, poniendo en conocimiento los riesgos materializados y atender las acciones que al respecto emita los miembros del Comité. • Realizar por lo menos una actividad de revisión y seguimiento obligatoria a los mapas de riesgos de los procesos, durante la vigencia, con la participación de los responsables para identificar posibles ajustes y cambios de los mapas. • Realizar seguimiento a partir de la revisión de los mapas de riesgos identificando si los controles se aplicaron, se materializo algún riesgo o hay algún reporte de no conformidades detectadas en las auditorias; en especial los institucionales y corrupción. Este seguimiento se hace a partir de la información reportada por la primera línea y puede ser realizado en las actividades de revisión de los mapas de riesgos. • Publicar los mapas de riesgos en la WEB • Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis y valoración del riesgo. • Asesorar a los líderes de procesos en la identificación de los riegos institucionales, de corrupción.
	Oficial de Seguridad de la información a cargo de la SSIT	• Asesorar a los líderes de proceso en la identificación de los riegos de seguridad de la información. • Presentar al Comité Institucional de Gestión y Desempeño, el seguimiento a la eficacia de los controles a los riesgos de seguridad de la información de los procesos. • Asesorar a los líderes de los procesos en la implementación de los controles definidos.
Tercera Línea	Oficina de Control Interno	• Asesorar de forma coordinada con la Oficina Asesora de Planeación y Prospectiva, a la primera línea de defensa en la identificación de los riesgos institucionales, de corrupción y de seguridad de la información y diseño de controles. • Llevar a cabo la evaluación independiente a los riesgos registrados en los mapas de riesgos de conformidad con el Plan Anual de Auditoría y reportar los resultados de la eficacia al Comité Institucional Coordinador de Control Interno. • Recomendar a la línea estratégica mejoras a la política de administración del riesgo.

2.4. Niveles de aceptación del riesgo y tratamiento

La agencia Nacional de tierras, establece que se realizará identificación de riesgos de seguridad de la información para los activos clasificados en criticidad alta, en relación a los activos de información clasificados en criticidad media o baja, se realizará un seguimiento de los mismos durante su vigencia para poder llevar un control de las posibles materializaciones de riesgos sobre estos activos que pueda llevar a cambiar su nivel de criticidad.

Una vez identificados y valorados los riesgos, la Agencia Nacional de Tierras acepta, solamente, los riesgos residuales en el nivel de exposición de riesgo "Bajo". En estos casos, no será necesaria la formulación del Plan de Acciones Preventivas para el diseño o fortalecimiento de controles. Los riesgos aceptados estarán sujetos a monitoreo por parte de la dependencia responsable del proceso.

En lo correspondiente a las categorías de tratamiento del riesgo y de acuerdo a la DEST-POLITICA-001 Política de administración del riesgo, la Agencia Nacional de Tierras adoptará los lineamientos metodológicos dispuestos por las autoridades administrativas competentes, los cuales serán confirmados según corresponda en el proceso de formulación o modificación al Mapa de Riesgos de seguridad de la información:

TRATAMIENTO	DESCRIPCIÓN	APLICACIÓN
Aceptar	No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción podrá ser aceptado).	Aplicar para riesgos inherentes y residuales en la zona de calificación de riesgo bajo.
Reducir	Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.	Aplica para riesgos residuales moderados, altos y extremos que pueden ser administrado mediante el diseño de nuevos controles o el fortalecimiento de los controles existentes, de modo que en el futuro el riesgo residual se pueda reevaluar como aceptable.
Evitar	Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.	Cuando los escenarios de riesgo identificado se consideran demasiado extremos y las actividades no están establecidas por la ley.
Compartir	Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad.	Cuando es muy difícil reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, este puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia, generalmente por medio de seguros o de tercerización.

Cuando se **materialice un riesgo** que fue previamente aceptado, se realiza la siguiente operación y determinar el desempeño del control:

$$1 - \left(\frac{\text{\# de enventos}}{\text{Frecuencia del riesgo}} \right)$$

- Número de eventos: # de eventos (Evento= es un riesgo materializado)
- Frecuencia del riesgo: Número de veces que se realiza la acción (# de veces que se realiza la acción)

Y con el resultado se debe proceder con alguna de las siguientes opciones:

1. Si el valor del resultado se encuentra entre el 100% y 90%, no se revisa el control - (Se mantiene)
2. Si el valor del resultado se encuentra entre el 90% y 80%, es potestad de la dependencia revisar el control - (Revisión de control)
3. Si el valor del resultado es inferior al 80%, se debe revisar el control para realizar ajustes (Cambio)

En el marco del seguimiento a la Administración de Riesgos de Gestión las dependencias responsables del proceso deben reportar a la Oficina de Planeación todas las materializaciones y los soportes correspondientes.

3. NORMATIVIDAD APLICABLE

El marco teórico que sustenta el procedimiento para la administración de riesgos en seguridad de la información es el siguiente:

1. Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 6 - noviembre de 2022.
2. Norma técnica Colombiana NTC-ISO/ IEC 27001: 2022 SISTEMAS DE GESTION DE SEGURIDAD DE LA INFORMACIÓN. Requisitos
3. Guía técnica colombiana GTC-ISO / IEC 27005: 2022 Orientaciones sobre la gestión de los riesgos para la seguridad de la información
4. Norma Técnica Colombiana NTC - ISO 9001. SISTEMAS DE GESTIÓN DE LA CALIDAD. Versión 2015
5. Norma Técnica Colombiana NTC -ISO 31000GESTIÓNDELRIESGO.DIRECTRICES
6. 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.
7. 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.
8. 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.

9. Guía de gestión de riegos, se adopta la Guía 7 de Gestión de Riesgos versión 3 de MinTIC, esta guía 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. Permite vincular la identificación y análisis de Riesgos de la Entidad hacia los temas de la Seguridad de la Información.

4. CONVENCIONES

Convenciones	Punto de Control	Actividades	
		Control	Riesgo
		© Texto en color azul	® Texto en color rojo

5. DESARROLLO DEL PROCEDIMIENTO

No.	Nombre Actividad	Descripción Actividad	Tiempo de ejecución	Dependencia Responsable
1.	Planificar y alistar los insumos necesarios para la identificación de riegos	Determinar los recursos necesarios para el procedimiento de identificación de riesgos 1. Inventario de activos de información. 2. Inventario de riesgos actuales 3. Resultados de seguimientos anteriores. 4. Programación de mesas técnicas	5 días	Subdirección de sistemas de información de tierras
		Asegurar la disponibilidad de los elementos necesarios desde las áreas estratégicas y operativas para la gestión y administración de los riesgos de seguridad de la información: *Elementos de planeación estratégica: Visión, Misión, Plan estratégico, FODA, Pestel, Contexto y Planes de acción. *Elementos de planificación operativa:		

2.	Establecer alcance y contexto	Inventario de activos de información, Mapa de procesos, Objetivos de los procesos y Caracterizaciones de procesos. *Lineamientos para la administración de riesgos en la entidad: • Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 6 DAFP • DEST-Política-001 Política de Administración del Riesgo • DEST–P-011 Procedimiento para la administración de riesgos de seguridad de la información • INTI-Política-001 Política General de Seguridad y Privacidad de la Información • DEST-F-004 Mapa de Riesgos de Seguridad de la Información	1 día	Subdirección de sistemas de información de tierras
3.	Establecer criterios de evaluación de riesgos	Identificar los criterios de valoración de riesgos de seguridad de la información, mediante el uso de la forma. DEST-F-004 Mapa de Riesgos de Seguridad de la Información en la hoja 0 – Criterios	1 día	Subdirección de sistemas de información de tierras
4.	Identificar el riesgo ®	Establecer en DEST-F-004 Mapa de Riesgos de Seguridad de la Información, Hoja 3-Identificación del Riesgo los datos requeridos y de acuerdo a la DEST-I-004 Instructivo Para la Identificación y Valoración de Riesgos de Seguridad de Información y Verificación de Controles Existentes	Inmediatamente después al establecimiento de los criterios para la evaluación de riesgos	Subdirección de sistemas de información de tierras – Dependencias ANT
5.	Valorar el Riesgo inherente	Una vez determinado el proceso, los activos de información, el responsable del proceso y la descripción del riesgo, se procede con la valoración del riesgo en DEST-F-004 Mapa de Riesgos de Seguridad de la Información, Hoja 4-Valoración del Riesgo, y de acuerdo a la DEST-I-004 Instructivo Para la Identificación y Valoración de Riesgos de Seguridad de Información y Verificación de Controles Existentes.	Inmediatamente después a la identificación del riesgo	Subdirección de sistemas de información de tierras – Dependencias ANT

6.	Verificar Controles Existentes ®	Hecha la valoración del riesgo inherente se debe proceder al análisis y verificación de la eficacia de los controles en DEST-F-004 Mapa de Riesgos de Seguridad de la Información, Hoja 5-Controles y de acuerdo a la DEST-I-004 Instructivo Para la Identificación y Valoración de Riesgos de Seguridad de Información y Verificación de Controles Existentes	Inmediatamente después a la valoración del riesgo	Subdirección de sistemas de información de tierras – Dependencias ANT
7.	Elaborar Matriz de riesgos de seguridad de la información	Realizada la identificación y valoración de controles existentes, se debe consolidar la información en la matriz de riesgos, con el objetivo de obtener el mapa de riesgos de seguridad de la información en DEST-F-004 Mapa de Riesgos de Seguridad de la Información, Hoja 6-Mapa de Riesgos Seguridad 1. Revisar que los valores generados en la hoja 6 Mapa Riesgos de Seguridad sean coherentes con la información ya registrada y generada. 2. Definir el indicador del control, en la columna Q. 3. Proyectar las acciones preventivas que permitan el control y manejo del riesgo, estableciendo responsable, indicador y fecha de ejecución.	Inmediatamente después a la verificación de controles	Subdirección de sistemas de información de tierras
8.	Formular plan de acciones preventivas ®	Registrar las acciones proyectadas en DEST-F-004 Mapa de Riesgos de Seguridad de la Información, hoja ANEXO 3 - Reporte Desempeño Acciones Preventivas, para el seguimiento a la ejecución de las mismas, de tal forma que se fortalezca el control de los riesgos y la mitigación de los mismos. Se debe tener en cuenta que, si el resultado de la solidez individual está por debajo del 96% se deben establecer acciones preventivas, este proceso deberá tener en cuenta la DEST-Política-001 Política de Administración del Riesgo, así como los criterios de evaluación establecidos en este procedimiento. Las acciones preventivas deben contener: • Acción preventiva • Responsable de la acción • Indicador de la acción • Cantidad Programada • Cantidad Lograda • Mes de ejecución	Inmediatamente después a la verificación de controles	Subdirección de sistemas de información de tierras – Dependencias ANT

		• Evidencia • Observaciones		
9.	Informar resultado de evaluación del riesgo de seguridad de la información y la propuesta de tratamiento de los mismos	Informar a la Oficina de Planeación, mediante correo electrónico los resultados de la evaluación del riesgo y las acciones establecidas para el tratamiento de los mismos. La información debe remitirse completa, con el cumplimiento de las tareas descritas en este procedimiento y manteniendo la integridad del mismo.	Inmediatamente después a la elaboración de la matriz de riesgos	Subdirección de sistemas de información de tierras
10	Revisar la pertinencia y verificar la calidad del resultado informado por la dependencia encargada de la seguridad de la información ©	La Oficina de Planeación revisa la pertinencia y verifica la calidad del resultado informado en relación a la evaluación de los riesgos de seguridad de la información y sobre la propuesta de tratamiento de los mismos, resultante de las tareas realizadas desde la identificación hasta la formulación de acciones preventivas La pertinencia se refiere a que el resultado informado sea Oportuno, Adecuado y Conveniente para la entidad. **Resultado Oportuno**: Contiene Controles y Acciones Preventivas que, desde la capacidad operativa, presupuestal y funcional, son viables de realizar en el momento en que se aprueba. **Resultado adecuado:** facilita a la entidad el cumplimiento de requisitos legales, normativos o reglamentarios y no contradice o genera incumplimientos en las funciones legalmente asignadas a las dependencias por el Decreto 2363 de 2015 y por las disposiciones adicionales de la Dirección General. **Resultado conveniente:** está directamente relacionado con una actividad del proceso al cual se atribuye y que resuelve la necesidad de mantener su operación bajo condiciones controladas. **Resultado de calidad:** cumple con las características técnicas establecidas en este procedimiento y con los criterios establecidos en la Forma: DEST-F-004 Mapa de Riesgos de Seguridad de la Información Cuando se aprueba el resultado se da continuidad a este procedimiento, de lo contrario la oficina de planeación, mediante correo electrónico, remite el resultado al área encargada de la seguridad de la información para que se	Inmediatamente después a la elaboración de la matriz de riesgos	Oficina de planeación

		realicen las correcciones correspondientes al criterio y tarea que se incumple. Los criterios y resultados de tareas no aprobadas se especificarán en esta misma comunicación. NOTA: Cuando la Oficina de Planeación desaprueba el resultado del ejercicio, se debe iniciar nuevamente el proceso, que incluya la revisión de toda la información generada desde la identificación del riesgo, con énfasis en la corrección de la o las tareas que se especifican como no aprobadas.		
11	Comunicar riesgo ©	1. Socializar el Mapa de Riesgos de seguridad de la información ante el Comité de gestión y desempeño. 2. Socializar los resultados aprobados de la evaluación y tratamiento de los riesgos asociados a sus procesos, al personal responsable de ejecutar actividades. 3. Brindar entrenamiento a funcionarios y contratistas, en la implementación de sus correspondientes actividades de Control. Según aplique, las actividades de socialización y entrenamiento se deben registrar en las formas dispuestas para tal fin en el proceso Gestión del Talento Humano o en el proceso Inteligencia de la Información: • GTHU-F-023- Forma Registro de Asistencia a Eventos de Formación • GTHU-F-025- Forma Entrenamiento en Puesto De Trabajo • INTI-F-008- Forma Para Elaborar Acta Reunión • INTI-F-009 Forma Listado de Asistencia	Inmediatamente después a la aprobación por parte de la oficina de planeación	Subdirección de sistemas de información de tierras
12	Ejecutar actividades de control ®	Una vez comunicados los riesgos y las acciones de tratamiento para los mismos, se deben establecer, cronogramas para el manejo y la verificación del cumplimiento de los controles: 1. Diseñar cronogramas de verificación de controles. 2. Registrar datos de verificaciones desarrolladas, en DEST-F-004 Mapa de Riesgos de Seguridad de la Información ANEXO 4 - Cronograma y Registro de Seguimiento **3.** Establecer acciones de mejora en relación a los datos obtenidos mediante las verificaciones,	Inmediatamente después a la aprobación por parte de la oficina de planeación y con	Subdirección de sistemas de información de tierras – Dependencias ANT

		estableciendo adicional: responsable, indicador y fecha de ejecución, en DEST-F-004 MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN ANEXO 3 - REPORTE DESEMPEÑO ACCIONES PREVENTIVAS	una periodicidad mensual	
13	Monitorear y Valorar la materialización de riesgos de seguridad de la información ©	Las dependencias líderes de procesos, ejerciendo su rol de primera línea de defensa (gerencia operativa) deben auto administrar de manera directa los riesgos de seguridad de la información, también, mediante el monitoreo permanente de la Materialización de los riesgos. Cuando se materializa un riesgo que está siendo administrado, los responsables deberán informar a la SSIT, quienes darán las indicaciones de tratamiento e iniciarán el análisis correspondiente, de acuerdo al GINFO-P-011 PROCEDIMIENTO GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN, mediante el formato GINFO-F-028-Registro de Incidentes de Seguridad de la Información y la GINFO-G-006-Guía de Gestión de Incidentes de Seguridad de la Información. Se deberá registrar la información correspondiente en DEST-F-004 Mapa de Riesgos de Seguridad de la Información ANEXO 2 - REPORTE DE MATERIALIZACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN, para su seguimiento y control. Las acciones preventivas que allí se generen deberán registrase de manera integral en el DEST-F-004 Mapa de Riesgos de Seguridad de la Información ANEXO 3 - REPORTE DESEMPEÑO ACCIONES PREVENTIVAS	En el momento que se materialice el riesgo	Subdirección de sistemas de información de tierras – Dependencias ANT
14	Reportar la materialización de riesgos y el plan de acción a la oficina de planeación y de control interno ©	Reportar mensualmente a la Oficina de Planeación, vía correo electrónico, la materialización del riesgo identificada, adjuntando los soportes correspondientes: ANEXO 2 - REPORTE DE MATERIALIZACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN. Cuando apliquen, las propuestas de actualización de Acciones Preventivas originadas por la materialización de riesgos se deben formular y proponer en DEST-F-004 Mapa de Riesgos de Seguridad de la Información, hoja Anexo 3 Reporte Acciones Preventivas.	Mensualmente	Subdirección de sistemas de información de tierras

15	Monitorear y reportar el desempeño del proceso en la ejecución del Plan de Acciones Preventivas formuladas	Definidas las acciones preventivas para los riesgos de seguridad de la información, los lideres por proceso junto con la SSIT, ejerciendo su rol de primera línea de defensa deberán ejecutar seguimiento sobre la ejecución de las mismas: 1. Diseñar cronograma de seguimiento a acciones preventivas. 2. Registrar datos de seguimiento y acciones de mejora identificadas. 3. Reportar mensualmente a la Oficina de Planeación, vía correo electrónico, la ejecución de las acciones preventivas, adjuntando los soportes correspondientes.	De acuerdo al cronograma establecido para seguimiento, con una periodicidad mensual	Subdirección de sistemas de información de tierras – Dependencias ANT
16	Realizar seguimiento a la administración de riesgos de seguridad de la información ©	Una vez implementadas las tareas de formulación y Seguimiento del DEST–P-011 Procedimiento para la administración de riesgos de seguridad de la información, la SSIT de la información deberá: 1. Elaborar informe de administración de los riesgos, teniendo en cuenta incluir: • Activos inventariados en el período. • Riesgos de seguridad identificados en el período. • Seguimiento a implementación de controles. • Estadísticas de Materialización de riesgos. • Seguimiento a acciones preventivas establecidas. • Información sobre valoraciones implementadas dada la materialización de los riesgos. • Capacitaciones y Socializaciones realizadas, en temas inherentes a seguridad de la información, con estadísticas de cobertura y eficacia. • Acciones de mejora de acuerdo a informe elaborado. 2. Presentar los informes solicitados por la Oficina de Planeación siguiendo la metodología establecida, usando los instrumentos establecidos y con los correspondientes soportes, sobre: • Los riesgos materializados en el periodo a reportar,	Anual	Subdirección de sistemas de información de tierras

		• Las propuestas de mejora en las Acciones Preventivas cuando se reportan riesgos materializados • El desempeño en la ejecución de las Acciones preventivas. En caso de presentarse alguna observación y antes de registrarse los informes, la Oficina de Planeación solicitará al responsable del riesgo realizar una mesa de trabajo para la revisión de novedades sobre el Plan de Acciones Preventivas y/o Materialización de Riesgos. NOTA: El informe de Seguimiento a la Administración de Riesgos de seguridad de la información, servirá como insumo para el Comité Institucional de Coordinación de Control Interno-CICCI, presentando la gestión realizada durante la vigencia, el Índice de Gestión del Riesgo y las oportunidades de mejora con base al cumplimiento de la Política de Administración del Riesgo de la ANT.		
17	Evaluar la eficacia de los controles ©	En el marco del Plan Anual de Auditoría, la Oficina de Control Interno evalúa la eficacia de los procesos en: • Ejecución de los Controles planificados • Implementación del Plan de Acciones Preventivas planificadas para fortalecer los controles para la mitigación del riesgo como resultado de la evaluación, La Oficina de Control Interno genera un informe con recomendación(es) a las dependencias en la prevención y tratamiento de los riesgos que puedan afectar el logro de sus objetivos. NOTA: la Oficina de Control Interno, realiza una muestra a los controles para su verificación y seguimiento, dado que las evidencias de estos controles los mantiene el responsable del riesgo en cada dependencia, dando cumplimiento a la Gestión Documental.	De acuerdo a cronograma de auditorías	Oficina Control interno
		La Oficina de Control Interno, en el marco del Plan Anual de Auditoría Interna, realiza actividades de evaluación con el propósito de confirmar si la Administración de riesgos ha tenido efecto positivo en el desempeño de Procesos, Planes, Programas y Proyectos. Las confirmaciones se basan en:	De acuerdo a cronograma de auditorías	Oficina Control interno

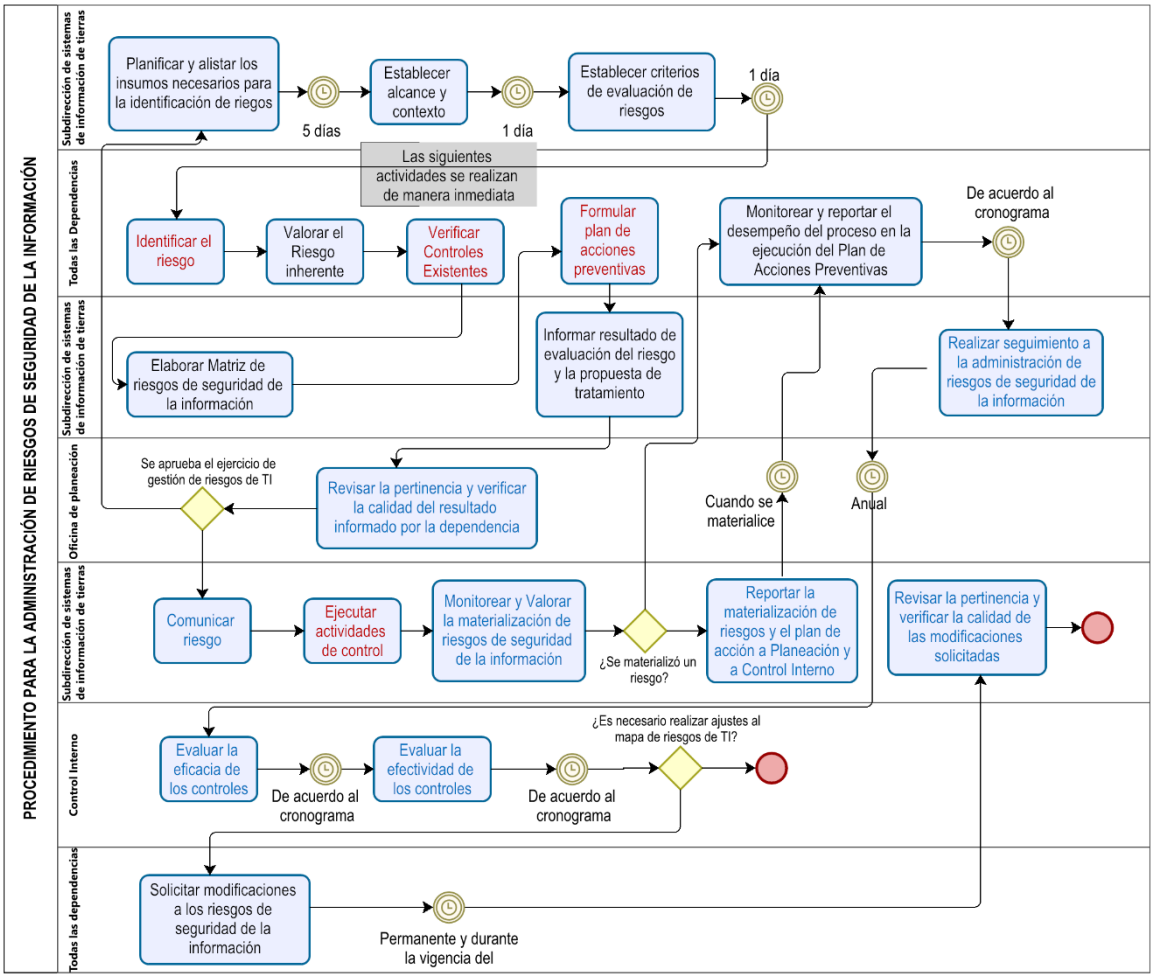
18	Evaluar la efectividad de los controles ©	Línea estratégica: Que la Política, Procedimientos e Instrumentos Para la de Administración de Riesgos sean acordes al contexto de la entidad. Primera línea de defensa: *Que los riesgos hayan sido identificados, evaluados y tratados de conformidad con la Política, Procedimientos e Instrumentos para la Administración de Riesgos. *Que los Controles estén bien diseñados, que se Ejecuten de manera consistente y que el responsable del proceso lleve a cabo las confirmaciones correspondientes a la gerencia operativa. Segunda línea de defensa: Que la Oficina de Planeación realice el seguimiento al Plan de Acciones Preventivas y Materialización de Riesgos y que Proporcione los métodos e instrumentos para la adecuada Administración de Riesgos Gestión en la entidad.		
19	Solicitar modificaciones a los riesgos de seguridad de la información y a los resultados de la evaluación y tratamiento	Durante la vigencia, las dependencias responsables de los Riesgos de seguridad de la información pueden solicitar modificaciones de forma o de fondo en la información correspondiente a los resultados de la evaluación de los riesgos y sus tratamientos, registrados en la versión vigente del Mapa de Riesgos de seguridad de la información. Las modificaciones deben cumplir criterios de calidad y pertinencia, que se refiere a que las modificaciones sean Oportunas, Adecuadas y Convenientes para la entidad. 1. Modificaciones Oportunas: contienen Diseño de Actividades de Control y Plan de Acción que, desde la capacidad operativa, presupuestal y funcional, son viables de realizar en el momento en que se aprueban. 2. Modificaciones adecuadas: facilitan a la entidad el cumplimiento de requisitos legales, normativos o reglamentarios y no contradice o genera incumplimientos en las funciones legalmente asignadas a las dependencias por el Decreto 2363 de 2015 y por las disposiciones adicionales de la Dirección General. 3. Modificaciones convenientes: están directamente relacionadas con una actividad del proceso	Permanente y durante la vigencia del procedimiento	Dependencias ANT

		al cual se atribuye y resuelven la necesidad de mantener su operación bajo condiciones controladas. 4. Modificaciones de calidad: cumplen con las características técnicas establecidas en este procedimiento y con los criterios establecidos en la Forma: DEST-F-001 MAPA DE RIESGOS DE GESTIÓN. Las modificaciones se deben solicitar en el ANEXO 1 - Solicitud de modificaciones al Mapa de Riesgos de seguridad de la Información. .		
20	Revisar la pertinencia y verificar la calidad de las modificaciones solicitadas ©	La Subdirección de sistemas de información, revisa la pertinencia y verifica la calidad de las modificaciones solicitadas a los Riesgos de seguridad de la información y a los resultados de la evaluación y tratamiento. A continuación, se describen los principales criterios técnicos para generar conceptos de no admisión a las solicitudes de modificación: • Que la actividad a modificar se encuentre vencida o en curso de ejecución. • Que la modificación no cumpla con los criterios de pertinencia y calidad establecidas en este procedimiento. • Que la modificación no cumpla los criterios definidos en la Forma: DEST-F-004 MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN, en la hoja 0, CRITERIOS. • Que la modificación no cumpla criterios definidos en la Guía para administración del riesgo y el diseño de controles en entidades públicas, publicada por Función Pública, versión 6. • Que la modificación desconozca las disposiciones normativas vigentes. • Que la modificación no contribuya a la detección, prevención o mitigación del riesgo. Cuando se aprueba el resultado se devuelve a la tarea 7. Cuando no se aprueba, la SSIT envía por correo electrónico al responsable del riesgo de la dependencia el ANEXO 1 - Solicitud de modificaciones al Mapa de Riesgos de seguridad de la Información con la(s) justificación(es). Cuando no se aprueba, finaliza el procedimiento.	Inmediatamente después de la solicitud de modificación a los riesgos de gestión	Subdirección de sistemas de información de tierras

6. DOCUMENTOS ASOCIADOS

- DEST-Política-001 ADMINISTRACIÓN DEL RIESGO
- DEST–P-011Procedimiento para la administración de riesgos de seguridad de la información
- INTI-Política-001 POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
- DEST-F-004 MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN
- ANEXO 1 - SOLICITUD DE MODIFICACIONES AL MAPA DE RIESGOS DE GESTIÓN
- ANEXO 2 - REPORTE DE MATERIALIZACIÓN DE RIESGOS
- ANEXO 3 - REPORTE DESEMPEÑO ACCIONES PREVENTIVAS
- GINFO-P-011 PROCEDIMIENTO GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
- GINFO-F-028-Registro de Incidentes de Seguridad de la Información

7. DIAGRAMA DE FLUJO



HISTORIAL DE CAMBIOS		
Fecha	**Versión**	**Descripción**
19/09/2024	1	Creación del documento

Elaboró: Johanna Rincón Molina	**Revisó:** Andrea Linney Sierra Ladino	**Aprobó:** Diana Lucia Herrera Riaño
Cargo: Contratista	**Cargo:** Contratista	**Cargo:** Subdirectora de sistemas de información de tierras
Firma: ORIGINAL FIRMADO	**Firma:** ORIGINAL FIRMADO	**Firma:** ORIGINAL FIRMADO
Fecha: 28/08/2024	**Fecha: 12/09/2024**	**Fecha: 12/09/2024**

La copia, impresión o descarga de este documento se considera COPIA NO CONTROLADA y por lo tanto no se garantiza su vigencia.

La única COPIA CONTROLADA se encuentra disponible y publicada en la página Intranet de la Agencia Nacional de Tierras.