MANUAL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

AGENCIA NACIONAL DE TIERRAS

SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN DE TIERRAS

DICIEMBRE DE 2024

1. INTRODUCCION

La estrategia de Gobierno Digital en Colombia ha venido siendo implementado de manera sistemática y coordinada en todas las entidades públicas. En los últimos años, se han evidenciado cambios y avances en el uso y apropiación de la tecnología como herramienta que permite mejorar la gestión pública, la provisión de servicios y la transparencia, encaminados a cumplir las funciones del Estado.

El sistema de gestión de seguridad de la información de la ANT, está integrado a las políticas, lineamientos, procesos, instructivos, guías y mapas de riesgos con la finalidad de minimizar los riesgos en materia de seguridad de la información y atender de forma positiva los incidentes de seguridad de la información, mediante la implementación de un ciclo de mejora continua que permita dar respuesta a las necesidades del contexto de la ANT en cuestiones de seguridad de la información, así como a los indicares establecidos para el alcance de los objetivos institucionales.

2. OBJETIVO DEL DOCUMENTO

Explicar la forma como la Agencia analiza el entorno de seguridad de la información, gestiona los riesgos, realiza la planificación, ejecución, verificación y mejora continua de los controles de seguridad seleccionados para el tratamiento de los riesgos de seguridad de la información, implementa los requisitos legales y prácticas recomendadas para la preservación de la confidencialidad, integridad y disponibilidad de la información, y como se revisa y mejora la eficiencia, eficacia y efectividad de la seguridad de la información en todos los procesos institucionales.

El Manual del Sistema de Gestión de Seguridad de la Información (SGSI) de la Agencia Nacional de Tierras (ANT), es un documento de referencia que describe las actividades generales aplicadas por la entidad para mejorar la gestión de la Seguridad de la Información.

3. ALCANCE

Desde la identificación y análisis del contexto interno y externo a nivel de seguridad de la información de la entidad, desarrollando la identificación y valoración de activos de información, así como de los riesgos y controles asociados a estos y finaliza con la evaluación y mejora de la gestión de la seguridad de la información en todos los procesos institucionales.

4. DEFINICIONES

Los términos relacionados a continuación se encuentran relacionados con los aspectos generales de la Seguridad de la información y la ISO 27001, permiten además la comprensión del presente manual y la articulación del mismo con los procedimientos, políticas, instructivos, manuales entre otros documentos que hacen parte integral del Sistema de gestión de Seguridad de la Información.

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis del riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo

ANT: Agencia Nacional de Tierras

Autorización: Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.

Base de Datos: Conjunto organizado de datos personales que sea objeto de tratamiento.

Ciberdefensa: Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional.

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

Cibernética: Ciencia de los sistemas de control y comunicación basados en retroalimentación, soportados o impulsados por la computación, particularmente en su relación con los seres vivos y el ser humano.

Ciberdelito / Delito Cibernético: Actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito.

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. Norma ISO/IEC 27000

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. Norma ISO/IEC 27000

Documento: Son documentos los escritos, impresos, planos, dibujos, cuadros, mensajes de datos, fotografías, cintas cinematográficas, discos, grabaciones magnetofónicas, videograbaciones, radiografías, talones, contraseñas, cupones, etiquetas, sellos y, en general, todo objeto mueble que tenga carácter representativo o declarativo, y las inscripciones en lápidas, monumentos, edificios o similares. Código General del Proceso, Ley 1564 de 2012, Artículo 243. Distintas clases de documentos.

Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y tratamiento de riesgos.

Identificación del riesgo: Proceso para encontrar, reconocer y describir riesgos.

Impacto: El costo para la empresa de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros p.ej., pérdida de reputación, implicaciones legales, etc.

Información: se refiere a un conjunto organizado de datos contenido en cualquier documento que la Entidad genere, obtenga, adquiera, transforme o controle. Ley 1712 de 2014, Transparencia y Derecho de acceso a la información pública

Integridad: Propiedad de precisión y completitud de la información.

MSPI: Sigla del Modelo de seguridad y privacidad establecido por el MINTIC en el marco de la estrategia de Gobierno Digital.

OTIC: Sigla de la Oficina de Tecnología de la Información y la Comunicación perteneciente al Ministerio de Salud y Protección Social.

Probabilidad: Posibilidad de que ocurra algo.

Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos. [Ley 1581 de 2012]

Riesgo de seguridad de la información: El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización.

SGSI: Sigla del Sistema de Gestión de Seguridad de la Información

Titular: Persona natural cuyos datos personales sean objeto de tratamiento. [Ley 1581 de 2012]

Transferencia: La transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país. [Ley 1581 de 2012]

Transmisión: Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable. [Decreto 1377 de 2013]

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. [Ley 1581 de 2012]

Tratamiento de riesgos: Proceso de modificar el riesgo, mediante la implementación de controles

Usuario: Todo servidor público, contratista, ente regulador, socios de negocios, y terceros entre otros que estén involucrados con información del Ministerio de Salud y Protección Social.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

5. REFERENCIAS NORMATIVAS Y DEFINICIONES

5.1. Normatividad

Para una adecuada gestión de la seguridad de la información, la Agencia Nacional de Tierras, tomó como base las recomendaciones del Modelo de Seguridad y Privacidad de la Información (MSPI) de la estrategia de Gobierno Digital del Ministerio de las Tecnologías de Información y las Comunicaciones - MINTIC, las políticas y normas del estado colombiano en materia de seguridad digital2 y la norma técnica Colombiana NTC ISO/IEC 2700.

Ahora bien, en concordancia con estos lineamientos la ANT verifica y actualiza de manera continua el NORMOGRMA INSTITUCIONAL en su sección de Seguridad de la información y el cual se puede encontrar en la página web de la entidad, en paralelo y a nivel interno se hace una verificación del cumplimiento que permite el registro de las acciones o documentos que permiten dicho cumplimiento normativo.

6. CONTEXTO DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

6.1. Contexto interno y Externo

La Agencia Nacional de tierras es una entidad pública que como lo establece el decreto 2363 de 2015 "*es la máxima autoridad de las tierras de la Nación y tendrá por objeto ejecutar la política de ordenamiento social de la propiedad rural formulada por el Ministerio de Agricultura y Desarrollo Rural, para lo cual deberá*

gestionar el acceso tierra como factor productivo, lograr la seguridad jurídica sobre ésta, promover su uso en cumplimiento de la función social de la propiedad y administrar y disponer de los predios rurales de propiedad de la Nación".

Dentro de este mismo ámbito la ANT cumple con funciones, que permiten el desarrollo estratégico de la misma:

1. Ejecutar las políticas formuladas por el Ministerio de Agricultura y Desarrollo Rural, sobre el ordenamiento social de la propiedad rural.
2. Ejecutar procesos de coordinación para articular e integrar las acciones de la Agencia con las autoridades catastrales, la Superintendencia de Notariado y Registro, y otras entidades y autoridades públicas, comunitarias o privadas de acuerdo con las políticas y directrices fijadas por el Ministerio de Agricultura y Desarrollo Rural.
3. Implementar el Observatorio de Tierras Rurales para facilitar la comprensión de las dinámicas del mercado inmobiliario, conforme a los estudios, lineamientos y criterios técnicos definidos por la Unidad de Planificación de Tierras Rurales, Adecuación de Tierras y Usos Agropecuarios -UPRA y adoptados por el Ministerio de Agricultura y Desarrollo Rural.
4. Ejecutar en las zonas definidas por el Ministerio de Agricultura y Desarrollo Rural, en la modalidad de barrido, los programas constitutivos de la política de ordenamiento social de la propiedad rural conforme a las metodologías y procedimientos adoptados para el efecto.
5. Apoyar la identificación física y jurídica de las tierras, en conjunto con la autoridad catastral, para la construcción del catastro multipropósito.
6. Validar los levantamientos prediales que no sean elaborados por la Agencia, siempre que sean coherentes con la nueva metodología de levantamiento predial del catastro multipropósito.
7. Ejecutar los programas de acceso a tierras, con criterios de distribución equitativa entre los trabajadores rurales en condiciones que les asegure mejorar sus ingresos y calidad de vida.
8. Otorgar el Subsidio Integral de Reforma Agraria, conforme a las políticas y lineamientos fijados por el Gobierno Nacional.
9. Administrar los bienes que pertenezcan al Fondo Nacional Agrario que sean o hayan sido transferidos a la Agencia.
10. Adelantar los procesos de adquisición directa de tierras en los casos establecidos en la Ley.
11. Administrar las tierras baldías de la Nación, adelantar los procesos generales y especiales de titulación y transferencias a las que haya lugar, delimitar y constituir reservas sobre éstas, celebrar contratos para autorizar su aprovechamiento y regular su ocupación sin perjuicio de lo establecido en los parágrafos 5 y 6 del artículo 85 de la Ley 160 de 1994.
12. Hacer el seguimiento a los procesos de acceso a tierras adelantados por la Agencia, en cualquiera de sus modalidades y aquellos que fueron ejecutados por el INCODER o por el INCORA, en los casos en los que haya lugar.
13. Verificar el cumplimiento de los regímenes de limitaciones a la propiedad derivadas de los procesos de acceso a tierras, de conformidad con la ley.
14. Delimitar y constituir las zonas de reserva campesina y zonas de desarrollo empresarial.
15. Administrar los fondos de tierras de conformidad con la ley y el reglamento.
16. Implementar y administrar el sistema de información de los Fondos de Tierras.

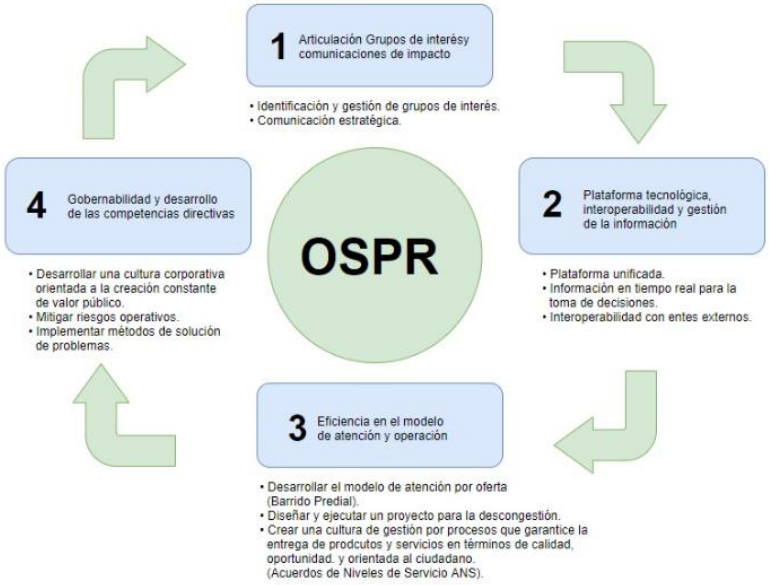
17. Implementar bases de datos y sistemas de información que permitan la articulación e interoperabilidad de la información de la Agencia con el Sistema Nacional de Gestión de Tierras.
18. Promover procesos de capacitación de las comunidades rurales, étnicas y entidades territoriales para la gestión de la formalización y regularización de los derechos de propiedad.
19. Administrar los bienes inmuebles extintos que fueron asignados definitivamente al INCODER por el Consejo Nacional de Estupefacientes con el objeto de implementar programas para el acceso a tierra a favor de sujetos de reforma agraria.
20. Gestionar la asignación definitiva de bienes inmuebles rurales sobre los cuales recaiga la acción de extinción de dominio administrados por el Fondo para la Rehabilitación, Inversión Social y Lucha contra el Crimen Organizado, FRISCO para destinarlos a los programas de generación de acceso a tierras, de acuerdo inciso 2 del artículo 91 de la Ley 1708 de 2014. Para la asignación definitiva se deberán seguir los lineamientos establecidos por el Comité de que tratan los artículos 2.5.5.5.4 y 2.5.5.11.3 del Decreto 2136 de 2015, una vez aprobada la asignación definitiva será la Agencia Nacional de Tierras la titular de la misma.
21. Impulsar, ejecutar y apoyar según corresponda, los diversos procedimientos judiciales o administrativos tendientes a sanear la situación jurídica de los predios rurales, con el fin de obtener seguridad jurídica en el objeto de la propiedad.
22. Gestionar y financiar de forma progresiva la formalización de tierras de naturaleza privada a los trabajadores agrarios y pobladores rurales de escasos recursos en los términos señalados en el artículo 103 de la Ley 1753 de 2015.
23. Asesorar a la ciudadanía en los procesos de transacción de predios rurales.
24. Adelantar los procedimientos agrarios de clarificación, extinción del derecho de dominio, recuperación de baldíos indebidamente ocupados, deslinde de tierras de la Nación, reversión de baldíos y reglamentos de uso y manejo de sabanas y playones comunales.
25. Concertar con las comunidades étnicas, a través de sus instancias representativas, los respectivos planes de atención.
26. Ejecutar el plan de atención a las comunidades étnicas, a través de programas de titulación colectiva, constitución, ampliación, saneamiento y reestructuración de resguardos indígenas, adquisición, expropiación de tierras y mejoras.
27. Adelantar los procesos agrarios de deslinde y clarificación de las tierras de las comunidades étnicas.
28. Delegar, en los casos expresamente autorizados en el artículo 13 de la Ley 160 de 1994, el adelantamiento de los procedimientos de ordenamiento social de la propiedad rural asignados a la Agencia.
29. Las demás funciones que le señale la ley, que por su naturaleza le correspondan.

Ahora bien, a través de las actividades de gestión de riesgos y oportunidades y planeación estratégica institucional del proceso de DIRECCIONAMIENTO ESTRATÉGICO (DEST-Caracterización), la Agencia Nacional de Tierras analiza su contexto interno y externo para comprender integralmente su contexto y así determinar los lineamientos estratégicos en materia de seguridad de la información.

En este ámbito la ANT cuenta con un direccionamiento estratégico que permite la articulación de cada una de las dependencias, funciones y requisitos con los objetivos de la entidad:

1. Misión: Como máxima autoridad de tierras, consolidar y mantener el ordenamiento social de la propiedad rural, para mejorar las condiciones de vida de la población.
2. Visión: Para el año 2030 la Agencia Nacional de Tierras habrá ordenado socialmente todo el territorio rural del país.
3. Ejes estratégicos

Gráfico 1. Ejes estratégicos -Agencia Nacional de Tierras



Fuente: Pagina Web – Agencia Nacional de Tierras.

- A nivel externo, entre otros, la Agencia estudia: factores sociales, culturales, políticos, legales, regulatorios, financieros, tecnológicos, económicos en los entornos internacionales, nacionales o locales, tendencias tecnológicas, necesidades y expectativas de las partes interesadas, para lograr un entendimiento de su posición externa en materia de seguridad de la Información.

- A nivel interno la entidad contempla su modelo de gobierno de la tecnología, su estructura organizacional, roles y responsabilidades respecto a la seguridad de la información, políticas, lineamientos y procesos internos de gestión institucionales, capacidades de sus recursos humanos y técnicos, expectativas y necesidades de sus partes interesadas internas, cultura organizacional, sistemas de información, flujos de información y relaciones contractuales entre otros.

De esta forma, para el SGSI se desarrolla un análisis del contexto interno y externo mediante la implementación de una matriz FODA y una matriz Pestel que permita el análisis de factores como:

Matriz FODA

- Fortalezas: acciones internas de la ANT que permiten la mejora continua de sus procesos y el alcance de objetivos a todos los niveles
- Oportunidades: Factores externos sobre los cuales no se tiene control, pero que mediante el accionar de estrategias a nivel interno permiten el fortalecimiento de la entidad.
- Debilidades: Elementos internos que tiene grandes oportunidades de mejora y que están afectando la entidad
- Amenazas: Factores externos que pueden ocasionar daño a las estrategias de la entidad y por ende al alcance de sus objetivos

Matriz PESTEL

- Político: indican de qué forma las acciones y medidas del gobierno pueden influir en la operatividad y rendimiento de la entidad
- Económico: Variables macroeconómicas que afectan el desempeño de la entidad
- Social y Cultural: aspectos tales como la creencia, cultura, religión, costumbres y preferencias de cada individuo, que puede influir en los procesos de la entidad.
- Tecnológico: Aspectos tecnológicos que, por su contante cambio y actualización, repercuten fácilmente en el contexto de la entidad y en sus procesos.
- Ecológico o ambiental: Factores ambientales que pueden ocasionar cambios el proceso de la entidad
- Legal: normativas y leyes que las entidades están obligadas a cumplir y respetar y que son insumo para el desarrollo de procesos, proyectos y planes.

Una vez elaborados estas herramientas se consolidará la información en el formato establecido por la ANT para los riesgos de seguridad de la información DEST-F-004 Mapa de Riesgos de Seguridad de la Información en la hoja 2-Contexto

6.2. Comprensión de las necesidades y expectativas

A fin de identificar y comprender las necesidades y expectativas de sus partes interesadas, la Agencia Nacional de Tierras aplica la política de participación ciudadana y ejecuta las actividades de gestión para la transparencia y direccionamiento del servicio al ciudadano del proceso de comunicación y gestión con grupos de interés. Sumado a esto se identifican las partes interesadas con el objetivo de mantener actualizada la información y dar cumplimiento a los requerimientos de las mismas.

Tabla 1. Grupos de Interés Agencia Nacional de Tierras

GRUPO DE INTERÉS	NECESIDADES Y EXPECTATIVAS
Ministerio de Agricultura y Desarrollo Rural	Rector de la Política Agraria en Colombia
Departamento Administrativo de Nacional *de Planeación*	Garantiza la adecuada formulación y ejecución de los proyectos de inversión
Ministerio de Hacienda y Crédito Público	Garantizar los recursos necesarios para la adecuada formulación y ejecución de los Planes Institucionales

Superintendencia de Notariado y Registro	Registrar los títulos para la formalización de la propiedad privada rural y los títulos que otorgan
Rama Judicial - Consejo Superior de la Judicatura	Interponer demandas para que se decida sobre la formalización de la propiedad privada rural.
Entidades del Sector Agrario Adscritas al MADR	Garantizar y coadyuvar la implementación de la política de Desarrollo Rural
Organizaciones sin ánimo de lucro	Cumplir con la función social que se establece dentro de su objeto misional, apoyando las comunidades étnicas
Alcaldías locales, Procurador ambiental y agrario local	Garantizar que las legalizaciones y compra de predios cumplan con la ley
Campesinos y organizaciones campesinas	Lograr que la ANT legalice sus territorios y adquirir predios para su desarrollo
Comunidades étnicas	Lograr que la ANT legalice sus territorios
Consejo Directivo - Agencia Nacional de Tierras	Contribuir al cumplimiento del objeto misional de la entidad
Administraciones departamentales y municipales	Fortalecen su economía mediante la diversificación productiva y de ingresos rurales a través de la constitución de las Zonas de Reserva Campesina

Fuente: Oficina de Planeación – Agencia Nacional de Tierras. Elaboración propia.

6.3. Alcance de la Gestión de la Seguridad de la información

El sistema de gestión de seguridad de la información de la Agencia Nacional de Tierras se aplica a todos los procesos estratégicos, misionales, de apoyo y de evaluación y control en sus sedes y UGT a nivel nacional.

6.4. Gestión de la Seguridad de la información en la Agencia Nacional de Tierras

La adopción del sistema de gestión de seguridad de la información, sus lineamientos, políticas, procedimientos y controles obedecen a decisiones estratégicas que se analizan, diseñan e implementan para satisfacer: necesidades expectativas, objetivos y requisitos legales. La Agencia Nacional de Tierras estableció, implementó, mantiene y mejora la gestión de la seguridad de la información en todos sus procesos institucionales a través de su sistema de gestión de seguridad de la información dentro del marco de su sistema integrado de gestión.

El sistema de gestión de seguridad de la información debe ser conocido y difundido a todos los funcionarios, contratistas y partes interesadas de la Agencia, el cumplimiento de lineamientos, políticas, procedimientos y controles es una obligación de todos los colaboradores independientemente de sus cargos, jerarquías, niveles de responsabilidad, o tipos de vinculación con la entidad.

7. LIDERAZGO Y COMPROMISO

7.1. Liderazgo

La alta dirección de la Agencia Nacional de Tierras demuestra su liderazgo y compromiso con la gestión de la seguridad de la información mediante:

a) Establecimiento de la política general de la seguridad de la información de la entidad
b) Asegurando que los requisitos de la gestión de la seguridad de la información estén incorporados al Sistema Integrado de Gestión Institucional.
c) Asegurando la existencia de los recursos humanos, económicos y técnicos necesarios para la gestión adecuada de la seguridad de la información en la Entidad.
d) Garantizando que se incluyen en los planes de comunicaciones institucionales la importancia de la gestión de la seguridad de la información y la necesidad de mantener la conformidad con los requisitos de seguridad institucionales
e) Evaluando los resultados de la gestión de la seguridad mediante la revisión periódica del sistema integrado de gestión
f) Dirigiendo y orientando a los funcionarios, contratistas y terceras partes interesadas en la gestión de la seguridad para lograr la eficacia del sistema.
g) Fomentando y promoviendo la adopción de oportunidades de mejora en la gestión de la seguridad.
h) Designando y apoyando los roles necesarios para una adecuada gestión de la seguridad de la información.

7.2. Política General de Seguridad

La agencia Nacional de Tierras adopta la siguiente INTI-Política-001 POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

"La AGENCIA NACIONAL DE TIERRAS (en adelante ANT) 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".

Ahora bien, en concordancia con las obligaciones constitucionales y legales sobre la protección de datos personales, la Agencia Nacional de Tierras, está comprometida con adoptar todas las medidas a su alcance

para garantizar el derecho de hábeas data de las personas que utilizan sus servicios o los datos personales que por la naturaleza de sus funciones son procesados por la Entidad, es así que cuenta e implementa la política INTI-Política-011 POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES.

En esta misma línea la ANT implementa el documento interno INTI-Política-008 LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN, el cual está alineado con la Declaración de Aplicabilidad y en el cual se detallan los aspectos técnicos, organizacionales y operativos para la implementación de las políticas de seguridad de la información.

7.2.1. Aprobación de la Política de Seguridad de la Información

La Política de Seguridad y Privacidad de la Información ha sido definida y aprobada por la Alta Dirección, y en ella se establece de forma clara, las líneas de actuación en Seguridad de la Información alineadas con los objetivos de la entidad.

La Política de Seguridad y Privacidad de la Información es adecuada al propósito de la entidad, proporciona un marco de referencia para establecer los objetivos, requisitos y mejora continua para la Seguridad de la Información, y se encuentra disponible a todas las partes interesadas, se formalizó el acta No 3 del Comité Institucional de Gestión y Desempeño, desarrollado el día 7 de octubre de 2024, por medio de la cual se adoptan los principios y lineamientos de tecnologías de la información y comunicaciones de la Agencia Nacional de Tierras.

7.2.2. Revisión de las políticas para seguridad de la información

Las políticas de seguridad de la información, así como la documentación del SGSI serán sometidos a revisión y actualización con una periodicidad anual o cuando se presenten cambios significativos en el contexto interno y/o externo de la Entidad.

La actualización del Sistema de Gestión de Seguridad de la Información es dinámica, lo cual implica que constantemente se deben documentar las acciones realizadas en el marco de este. Por lo menos una vez al año se deben presentar al Comité de Seguridad o el que haga sus veces, los avances realizados.

Mínimo cada tres años se debe iniciar nuevamente las fases del ciclo PHVA de la implementación del Sistema de Gestión de Seguridad de la Información.

En paralelo a esto la revisión periódica de las políticas y la documentación del Sistema de Gestión de la Seguridad de la Información se deberá incluir en el proceso de SEGUIMIENTO EVALUACIÓN Y MEJORA, a través de la actividad Revisión por la Dirección al Desempeño Institucional.

7.3. Roles, responsabilidades y autoridades

La ANT asigna los roles y responsabilidades pertinentes a la gestión de la seguridad de la información así:

ROL	RESPONSABILIDADES	AUTORIDAD
Alta Dirección	•Aprobación de los alcances, políticas, lineamientos, normas, directrices y procedimientos, así como herramientas, manuales, modelos de operación, metodologías y estructuras organizacionales empleadas para la gestión del MSPI y seguimiento a su cumplimiento y actualización permanente. •Asegurar que el Sistema de Gestión de Seguridad de la Información se establezca, implemente y mantenga. •Gestión para la asignación de los recursos para establecer, implementar, operar hacer seguimiento, revisar, mantener y mejorar el MSPI institucional, para que las iniciativas relacionadas con la gestión de seguridad de la información se lleven a cabo y para que los lineamientos definidos se implementen. •Fomentar el cumplimiento de las políticas y lineamientos definidos en materia de seguridad de la información en los colaboradores de la Entidad. •Apoyar la difusión y sensibilización de la seguridad de la información en la Entidad. •Determinar como resultado de la revisión del SGSI, las decisiones y acciones relacionadas con la mejora en la eficacia del SGSI, la mejora del producto o servicio en relación con los requisitos del cliente y las necesidades de recursos	•Tomar las decisiones necesarias para el mantenimiento y mejora del SGSI •Aprobar los actos administrativos y documentos necesarios como compromiso de la Alta Dirección •Aprobar la asignación de recursos para el mantenimiento y mejora del SGSI •Designar responsabilidades relacionadas con el SGSI •Aprobar el informe de revisión por la alta dirección del SGSI y las acciones de mejora propuestas •Solicitar la implementación de modificaciones, mejoras y cualquier necesidad de cambio en el sistema integrado de gestión cuando lo considere pertinente •Solicitar al Oficial de Seguridad de la Información y demás áreas responsables la aplicación de los controles del SGSI •Requerir informes de gestión y evaluación del SGSI, cuando lo considere pertinente
Comité institucional de gestión y desempeño	•Revisar periódicamente las diferentes políticas o propuestas realizadas para el SGSI, aprobándolas o comunicando los ajustes a los que haya lugar •Realiza seguimiento al cumplimiento y actualización permanente de los alcances, planes, políticas, lineamientos, directrices y procedimientos, así como herramientas, manuales, modelos de operaciones, metodologías y estructuras organizacionales empleadas para la gestión del SGSI •Hacer seguimiento a las actividades de actualización a los perfiles de riesgo en Seguridad de la Información y protección de datos personales, así como a los planes de tratamiento de riesgo que surjan como resultado de dicha actualización. •Promover que todos los funcionarios vinculados a la entidad conozcan, entiendan y ejerzan sus responsabilidades frente al cumplimiento del SGSI •Revisión del proyecto de presupuesto relacionado con Seguridad de la Información y continuidad del negocio.	•Tomar decisiones para la mejora continua del SGSI •Requerir informes de gestión y evaluación del SGSI, cuando lo considere pertinente
Oficial de Protección de Datos	• Velar por el respeto de los derechos de los titulares de los daos personales respecto del tratamiento de datos que realice el prestador de servicios ciudadanos digitales. • Informar y asesorar el prestador de servicios ciudadanos digitales en relación con las obligaciones que les competen en virtud de la regulación colombiana sobre privacidad y tratamiento de datos personales. • Supervisar el cumplimiento de lo dispuesto en la regulación y en las políticas de tratamiento de información del prestador de servicios ciudadanos digitales, así como del principio de responsabilidad demostrada. • Prestar el asesoramiento que se le solicite acerca de la	• Tomar decisiones necesarias sobre la gestión y tratamiento de Datos Personales • Reportar las bases de Datos con información personal ante la Superintendencia de Industria y Comercio • Reportar los incidentes de Seguridad de la Información que comprometan datos personales ante la Superintendencia de Industria y Comercio

ROL	RESPONSABILIDADES	AUTORIDAD
	evaluación de impacto relativa a la protección de datos. • Atender los lineamientos y requerimientos que le haga la Delegatura de Protección de Datos Personales de la Supervisión de Industria y Comercio o quien haga sus veces.	
Oficial de Seguridad de la Información	• Formular las políticas, lineamientos, controles y procedimientos encaminados a fortalecer la seguridad de la información. • Identificar las necesidades de la Agencia Nacional de Tierras frente al Modelo de Seguridad y Privacidad de la Información de MinTic. • Identificar la brecha entre el SGSI de la información y la situación de la Agencia Nacional de Tierras. • Realizar el autodiagnóstico de Seguridad de la Información de la Entidad. • Coordinar y gestionar los incidentes de seguridad de la información que se presenten en la Entidad. • Realizar seguimiento y monitoreo a la gestión y tratamiento de Riesgos de Seguridad de la Información • Generar el Plan de Trabajo para la implementación y mantenimiento del SGSI, así como el plan de trabajo, entregables y seguimiento de cumplimiento del mismo.	- Reportar avances en cuanto al desempeño del SGSI al Comité d Gestión y Desempeño. - Reportar ante las entidades competentes los incidentes de seguridad de la información acontecidos en la Entidad
Equipo de Seguridad de la Información	•Análisis y gestión de riesgos en seguridad y privacidad Seguridad de la Información, y liderar coordinación de la gestión de la implementación de controles para su mitigación. •Velar por el cumplimiento normativo asociado a la seguridad y privacidad de la información. •Monitorear y medir del cumplimiento de políticas, lineamientos, normas, estándares y procedimientos en Seguridad y Privacidad de la Información y tratamientos para subsanar las vulnerabilidades identificadas. •Capacitar y sensibilizar en seguridad y privacidad de la información. •Regular la gestión de activos de información, teniendo en cuenta su clasificación y las medidas de seguridad pertinentes. •Monitorear la gestión de vulnerabilidades técnicas de seguridad informática. •Gestión de Incidentes de Seguridad y privacidad de la Información con el apoyo de los grupos involucrados. •Informar sobre los avances en el cumplimiento de las directrices de Seguridad y Privacidad de la Información y por los procedimientos y prácticas que de ellas surjan. •Seguimiento a los incidentes en Seguridad y Privacidad de la Información presentados. •Revisar periódicamente el estado del SGSI a partir de indicadores definidos. •Atender las auditorías internas y externas que se hagan al MSPI •Seguimiento a los resultados del monitoreo realizado a la gestión de Seguridad de la Información, a las medidas de mejoramiento adoptadas por resultados de auditorías internas y externas al SGSI	•Solicitar informes de cumplimiento de controles de seguridad. •Reportar incumplimientos de políticas de seguridad a la Alta Dirección •Autorizar actividades relacionadas con seguridad de la información
Oficina Asesora de control interno	•Ejecución de la auditoría al SGSI y a la conformidad y cumplimiento de los requisitos legales aplicables a la Entidad en relación con la Seguridad y Privacidad de la Información.	Requerir información sobre los soportes de implementación de los controles de SGSI

ROL	RESPONSABILIDADES	AUTORIDAD
	•Informar sobre el cumplimiento de las directrices de Seguridad de la Información en el marco de la norma vigente auditada. •Hacer seguimiento a los planes de mejoramiento resultado de las auditorías internas. •Informar los resultados de la auditoría interna al SGSI al Comité Institucional del Gestión y Desempeño.	
Talento Humano	•Implementar las políticas de seguridad y privacidad de la información asociadas al talento humano. •Gestionar las autorizaciones de tratamiento de datos personales de los funcionarios. •Incluir dentro de los procesos de inducción temas de seguridad y privacidad de la información. •Incluir dentro del plan anual de capacitación todos los temas referentes a seguridad y privacidad de la información. •Realizar convocatorias a las charlas, conversatorios y demás eventos programados que promuevan la concienciación en Seguridad y Privacidad de la Información, así como proveer los recursos para la respectiva ejecución del evento y su control de asistencia.	Escalar a control interno disciplinario las investigaciones por incumplimiento de políticas de seguridad de la información.
Oficina Jurídico	Determinación de la procedencia de abrir procesos disciplinarios por el incumplimiento de políticas y lineamientos de seguridad y privacidad de la información y/u ocurrencia de actos malintencionados que afecten la seguridad de la información que involucren a empleados públicos, trabajadores oficiales y/o contratistas, acorde con lo estipulado en el Código Único Disciplinario (Ley 734 de 2002), o las normas que lo modifiquen o complementen.	Abrir procesos disciplinarios a los funcionarios por incumplimiento de las políticas de seguridad de la información.
Todas las áreas de la Entidad, líderes y Colaboradores	•Conocimiento y cumplimiento de las disposiciones y lineamientos para la Seguridad de la Información establecidos en la entidad. •Asistencia a las capacitaciones y sensibilizaciones que programe la Entidad en temas de Seguridad de la Información •Reporte de eventos e incidentes de Seguridad de la Información y apoyo en la atención e investigación del mismos. •Apoyo en la respuesta a requerimientos internos y externos en materia de Seguridad de la Información. •Apoyo en la identificación y clasificación de activos de información y la realización de los análisis de riesgos y planes de tratamiento respectivos. •Definición y aplicación de mecanismos y controles para la protección de los activos de información.	Toma de decisiones sobre las actividades del proceso Gestionar los recursos necesarios para llevar a cabo las actividades El líder del proceso tiene la autoridad de aprobar la creación, modificación o eliminación de documentos del proceso, riesgos y cualquier cambio que se presente en el proceso.

8. PLANIFICACIÓN Y GESTIÓN DE RIESGOS DE SEGURIDAD

8.1. Gestión de riesgos de seguridad de la información

Las acciones para la gestión y tratamiento de riesgos de seguridad de la información se desarrollan mediante la aplicación de la Guía para la Administración de los riesgos de gestión, corrupción y seguridad digital y el diseño de controles en entidades públicas y mediante la aplicación del DEST–P-011 PROCEDIMIENTO ADMINISTRACION DE RIESGOS DE SEGURIDAD DE LA INFORMACION y el DEST-I-004 INSTRUCTIVO

PARA LA IDENTIFICACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y VERIFICACIÓN DE CONTROLES EXISTENTES.

Los resultados de las actividades de identificación, evaluación, valoración y tratamiento de riesgos se documentan en la matriz de riesgos DEST-F-004 MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

Las decisiones sobre los controles de seguridad de la información recomendados por la norma ISO 27001 y la Estrategia de Gobierno Digital, se consignan en la Declaración de Aplicabilidad de controles de seguridad de la información de la ANT.

8.2. Objetivo de la seguridad de la información

La Agencia Nacional de Tierras ha adoptado el siguiente conjunto de objetivos de la seguridad de la información, los cuales están alineados con los objetivos estratégicos institucionales y hacen parte integral de la Política de Seguridad y Privacidad de la Información:

- Implementar controles técnicos, administrativos y legales enfocados a la protección de la confidencialidad, integridad, disponibilidad de la información, así como mitigar eventos que generen impactos económicos, reputacionales y a nivel legal, conforme a la Declaración de Aplicabilidad de la Entidad.

- Sensibilizar, divulgar y comunicar a todos los colaboradores y usuarios de los sistemas de información de la Entidad, a fin de generar y fortalecer la cultura de seguridad de la información, incentivando la aplicación de buenas prácticas respecto al adecuado tratamiento y protección de los activos de información a los cuales tienen acceso.

- Gestionar las situaciones (incidentes y eventos) de seguridad de la información.

- Fortalecer la capacidad institucional para identificar, detectar, proteger, responder y recuperar ante ciberataques que puedan afectar la operación y los activos de información de la Entidad.

- Cumplir con las directrices del Ministerio de Tecnologías de la Información y Comunicaciones para la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI.

8.3. Planificación de los cambios

Cuando la ANT determine la necesidad de realizar cambios en el Sistema de Seguridad de la Información lo realizará de manera planificada y en el marco del cumplimiento legal y normativo descrito en el numeral 5.1 NORMATIVIDAD del presente documento.

9. RECURSOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD

9.1. Recursos

La Entidad determina periódicamente los recursos que son necesarios para gestión de la seguridad de la información a través de los resultados de la revisión de su sistema integrado de gestión, la cual se realiza en el proceso de EVALUACIÓN, SEGUIMIENTO Y MEJORA.

Los recursos para el direccionamiento estratégico de la seguridad de la información son administrados por el proceso de INTELIGENCIA DE LA INFORMACIÓN.

Los recursos para la gestión y operación de los controles de seguridad de la información de los diferentes procesos son administrados por el proceso de GESTIÓN DE INFORMACIÓN

Las tareas de gestión del talento humano necesario para el desarrollo y control de las actividades para de la seguridad de la información son coordinadas desde el proceso de GESTIÓN DE TALENTO HUMANO, y los procesos de ADQUISICIÓN DE BIENES Y SERVICIOS y ADMINISTRACIÓN DE BIENES Y SERVICIOS.

Los recursos necesarios para realizar el seguimiento, evaluación y mejora del sistema de gestión de la seguridad de la información son gestionados desde el proceso de EVALUACIÓN, SEGUIMIENTO Y MEJORA.

9.2. Competencia

La determinación de las competencias necesarias para las personas que realizan trabajos relacionados con la seguridad de la información se realiza a través del proceso de INTELIGENCIA DE LA INFORMACIÓN y teniendo en cuenta la aceptabilidad de los roles y responsabilidades establecidos para el SGSI.

Desde el proceso de INTELIGENCIA DE LA INFORMACIÓN mediante las actividades GESTIÓN DEL CONOCIMIENTO se identifica información y experiencias innovadoras, que generan buenas prácticas institucionales, esto genera propuestas para mejorar el conocimiento de los colaboradores de la ANT en materia de seguridad de la información, estas oportunidades son comunicadas al proceso de TALENTO HUMANO, quien ajusta anualmente el PLAN DE ACCIÓN ANUAL en el componente de capacitación (Plan Institucional de Capacitación)

9.3. Toma conciencia

La toma de conciencia dentro de la ANT se desarrolla mediante la aplicación del Plan Institucional de Capacitación – PIC, de igual forma mediante el proceso de identificación de riesgos de seguridad de la

información, se definen planes de formación específicos para las dependencias de acuerdo con las necesidades evidenciadas y encaminadas al logro de los objetivos planteados para el SGSI.

Se deberá incluir como mínimo en los planes de capacitación específicos y en el PIC, los siguientes temas:

- Normatividad General.
- Política de Seguridad y Privacidad de la Información.
- Procedimientos, instructivos y lineamientos de seguridad de la Información de la ANT.
- Beneficios y ventajas de la implementación de buenas prácticas de seguridad de la Información.
- Implicaciones de las no conformidades con la norma ISO 27001 y los controles anexos a la misma.
- Que los funcionarios, contratistas y terceras partes interesadas conozcan cómo pueden contribuir la mejora del desempeño de la seguridad de la Entidad

9.4. Comunicación

Las comunicaciones internas y externas necesarias para la gestión de la seguridad de la información se socializan a través de los canales institucionales como correo electrónico, intranet, sitio web y redes sociales y otros canales de comunicación definidos por la Entidad.

9.5. Estructura de la Documentación

Este documento hace parte del sistema integrado de gestión de la ANT, todo el control de la documentación de la gestión de la seguridad se realiza mediante el procedimiento INTI-P-001 CONTROL DE LA INFORMACIÓN DOCUMENTADA V4.

El manual del Sistema de Gestión de la Seguridad de la Información se basa en los numerales y cláusulas de la norma NTC ISO/IEC 27001

10. OPERACIÓN

La planificación y control operacional del Sistema de Gestión de la Seguridad de la Información se realiza a través del sistema integrado de gestión, los procedimientos e instructivos específicos a la seguridad de la información se administran a través del proceso de GESTIÓN DE INFORMACIÓN e INTELIGENCIA DE LA IINFORMACIÓN.

La valoración y tratamiento de riesgos de seguridad de la información se soportan en las acciones recomendadas por la Guía para la Administración de los riesgos de gestión, corrupción y seguridad digital y el diseño de controles en entidades públicas del DAFP y en el DEST–P-011 PROCEDIMIENTO ADMINISTRACION DE RIESGOS DE SEGURIDAD DE LA INFORMACION y el DEST-I-004 INSTRUCTIVO

PARA LA IDENTIFICACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y VERIFICACIÓN DE CONTROLES EXISTENTES.

11. EVALUACIÓN DEL DESEMPEÑO

11.1. Seguimiento, Medición, Análisis y Evaluación

La evaluación del desempeño del Sistema de Gestión de la Seguridad de la Información de la información se realiza aplicando los mecanismos de seguimiento, medición, análisis y evaluación del proceso de SEGUIMIENTO, EVALUACIÓN Y MEJORA.

Para la evaluación de la eficacia de la gestión de la seguridad de la información se utilizan indicadores definidos por el proceso de DIRECCIONAMIENTO ESTRATÉGICO, a través del procedimiento GESTIÓN DE INDICADORES DEST-P-007. El cual igualmente permite realizar seguimiento de los indicadores aprobados.

De igual forma se hace seguimiento a las acciones preventivas establecidas y controles evaluados en la matriz de riesgos DEST-F-004 MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

11.2. Auditoría Interna

Las auditorias al Sistema de gestión de seguridad se realizan mediante el Procedimiento SEYM-P007, del PROCESO DE EVALUACIÓN, SEGUIMIENTO Y MEJORA

11.3. Revisión por la Dirección

La revisión del Sistema de Gestión de la Seguridad de la Información se realiza simultáneamente con la revisión por parte de la dirección del sistema integrado de gestión, en el proceso de EVALUACIÓN, SEGUIMIENTO Y MEJORA SEYM-Caracterización, los resultados de la gestión de la seguridad de la información son analizados desde del proceso DIRECCIONAMIENTO ESTRATÉGICO, con el procedimiento GESTIÓN DE INDICADORES DEST-P-007 con sus actividades de seguimiento de indicador y análisis del indicador

12. MEJORA

12.1. No conformidades y Acciones correctivas.

Las no conformidades y acciones correctivas para el Sistema de Gestión de la Seguridad de la Información se realizan a través de los procedimientos de CONTROL DE SALIDAS NO CONFORMES, SEYM-P-003.

12.2. Mejora continua.

La mejora continua del Sistema de Gestión de la Seguridad de la Información se coordina a través del proceso de SEGUIMIENTO EVALUACIÓN Y MEJORA con su procedimiento GESTIÓN DEL PLAN DE MEJORAMIENTO SEYM-P-002

13. DECLARACIÓN DE APLICABILIDAD

CONTROL ISO 27K:2022	OBJETIVO DEL CONTROL	APLICA	JUSTIFICACIÓN
A5. Controles Organizacionales			
A.5.1	Políticas para la seguridad de la información	Si	Se establece para dar cumplimiento a la norma ISO27001:2022 y al Modelo de Seguridad de la Información establecido por Mintic
A.5.2	Roles y Responsabilidades de la Seguridad de la Información	Si	Se acoge este control para garantizar la definición organizada del equipo de seguridad de la Información dentro de la Entidad
A.5.3	Segregación de tareas	Si	Se acoge este control para garantizar la definición organizada del equipo de seguridad de la Información dentro de la Entidad para evitar el conflicto de intereses dentro de la gestión del SGSI
A.5.4	Responsabilidades de la dirección	Si	Se acoge este control para garantizar el compromiso de la dirección con el SGSI.
A.5.5	Contacto con las autoridades	Si	Se acoge este control dado que ante la ocurrencia de incidentes de seguridad informática que se consideren graves o de difícil control relacionados con cualquier ataque cibernético, se deberán reportar al COLCERT y/o CSIRT para pedir el apoyo necesario del incidente que amerite ser tratado.
A.5.6	Contacto con grupos de interés especial	Si	Se acoge este control dado que ante la ocurrencia de incidentes de seguridad informática que se consideren graves o de difícil control relacionados con cualquier ataque cibernético, se deberán reportar al COLCERT y/o CSIRT para pedir el apoyo necesario del incidente que amerite ser tratado.
A.5.7	Inteligencia de amenazas	Si	Se acoge este control para garantizar la gestión de vulnerabilidades y las actividades de prevención de explotación de vulnerabilidades en la plataforma tecnológica de la ANT.
A.5.8	Seguridad de la información en la gestión de proyectos	Si	Se acoge este control para garantizar que toda la Entidad en la ejecución del proyecto considere los temas de Seguridad de la Información y ciberseguridad.
A.5.9	Inventario de información y otros activos asociados	Si	Se acoge este control para identificar los activos e inventario de información de interés de la ANT
A.5.10	Uso aceptable de la información y otros activos asociados	Si	Se acoge este control para asegurar el reconocimiento, documentación e implementación de las normas de documentación y clasificación de información estipuladas por la ANT.
A.5.11	Devolución de activos	Si	Se acoge este control debido a que en la ANT asegura el retorno del activo a su propietario o custodio en la finalización de la relación contractual
A.5.12	Clasificación de la información	Si	Se acoge este control dado que la ANT cuenta con mecanismos para la protección de la información mediante su adecuada calificación de acuerdo con los requisitos legales

CONTROL ISO 27K:2022	OBJETIVO DEL CONTROL	APLICA	JUSTIFICACIÓN
A.5.13	Etiquetado de la información	Si	Se acoge este control dado que la ANT cuenta con mecanismos para la protección de la información mediante su adecuada calificación de acuerdo con los requisitos legales
A.5.14	Transferencia de la información	Si	Se acoge este control dado que la ANT debe custodiar los canales y registros de información que es transferida con terceros.
A.5.15	Control de Acceso	Si	Se acoge este control dado que la ANT vigila y controla los accesos a los activos de información de la Entidad
A.5.16	Gestión de la identidad	Si	Se acoge este control dado que para la ANT la administración de identidades es vital como mecanismo de seguridad para la autenticación.
A.5.17	Información de autenticación	Si	Se acoge este control dado que la información de autenticación permite la identificación y control de usuarios para la adecuada gestión de acceso a sistemas y aplicaciones de la Entidad.
A.5.18	Derechos de acceso	Si	Se acoge este control como regla para los roles de usuario específicos en relación con los activos de información de la ANT.
A.5.19	Seguridad de la información en la relación con proveedores	Si	Se acoge este control ya que para la ANT es relevante establecer relaciones y control seguro con los proveedores que tienen acceso a los activos de información de la Entidad.
A.5.20	Requisitos de seguridad de la información en contratos con terceros	Si	Se acoge este control dado que los terceros deben conocer desde las instancias iniciales de la relación contractual las condiciones de seguridad de la información impartidas por la ANT.
A.5.21	Gestión de la seguridad de la información en la cadena de suministro de las TIC (Tecnologías de Información y Comunicación)	Si	Se acoge este control dada la relevancia e importancia técnica que tiene la cadena de suministro de las TIC en la disponibilidad de la infraestructura tecnológica de la ANT, y su incidencia en los procesos institucionales.
A.5.22	Gestión del cambio, revisión y monitoreo de los servicios del proveedor o suministrador	Si	Se acoge este control dado que todo cambio que pueda afectar la disponibilidad y continuidad de los servicios institucionales debe ser gestionado de manera organizada, controlada y planificada al interior de la Entidad.
A.5.23	Seguridad de la Información para el uso de servicios en la nube	Si	Se acoge este control ya que la Entidad cuenta con plataforma tecnológica en nube en constante evolución y se deben considerar en todo momento las mejores prácticas de la industria para asegurar este ambiente.
A.5.24	Planeamiento y preparación de la gestión de incidentes de seguridad de la información	Si	Se acoge este control dado que la ANT debe realizar seguimiento y control organizado a los incidentes de seguridad de la información que se puedan llegar a presentar en la ANT.
A.5.25	Evaluación y decisión en los eventos de seguridad de la información	Si	Se acoge este control dado que la ANT debe evaluar y decidir sobre todos los eventos de seguridad de la información que se puedan presentar en la Entidad.
A.5.26	Respuesta a los incidentes de seguridad de la información	Si	Se acoge este control dado que la ANT debe dar respuesta a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados definidos por el equipo de Seguridad de la Información.
A.5.27	Aprendizaje sobre los incidentes de seguridad de la información	Si	Se acoge este control dado que la ANT debe formular planes de acción y remediación en base a las lecciones aprendidas de los incidentes para endurecer su postura de seguridad ante futuros ataques.
A.5.28	Recolección de evidencia	Si	Se acoge este control dado que la ANT debe recolectar y analizar la información asociada a los eventos e incidentes de seguridad de la información para reducir la posibilidad o el impacto de incidentes futuros por medio de las lecciones aprendidas.
A.5.29	Seguridad de la información durante interrupciones	Si	Se acoge este control dado que la ANT debe realizar los análisis de impacto al negocio y los análisis de riesgos de continuidad para formular estrategias de recuperación en caso de desastres y así preparar a las TIC para la continuidad del negocio.

CONTROL ISO 27K:2022	OBJETIVO DEL CONTROL	APLICA	JUSTIFICACIÓN
A.5.30	Preparación de las TIC para la continuidad de negocio	Si	Se acoge este control dado que la ANT debe gestionar la planeación e implementación de las estrategias de recuperación para los sistemas de información que apoyan los procesos misionales de la Agencia, a través del Plan de Recuperación de Desastres y Planes de Contingencia
A.5.31	Requisitos legales, estatutarios, regulatorios y contractuales	Si	Se acoge este control dado que la ANT se compromete con el cumplimiento de los requisitos legales y los estándares de seguridad establecidos por el Ministerio de las Tecnologías de la Información y las Comunicaciones a través de la política de Gobierno Digital.
A.5.32	Derechos de propiedad intelectual	Si	Se acoge este control considerando que la ANT da cumplimiento al artículo 91 de la ley 23 de 1982 sobre derechos de autor. Así mismo se encarga de asegurar que los sistemas de información adquiridos cuenten con un acuerdo de licenciamiento, el cual especifica las condiciones de uso del software y los derechos de propiedad intelectual.
A.5.33	Protección de registros	Si	Se acoge este control ya que para la ANT la conservación y protección de registros es relevante para la vigilancia y gestión adecuada de información, activos y accesos que puedan afectar los sistemas de información institucionales.
A.5.34	Privacidad y protección de la información de identificación personal PII	Si	Se acoge este control dado que para la ANT la custodia y debido tratamiento de la Información de Identificación Personal es realizada en el marco de la Ley 1581 de 2012 y según las disposiciones de la Superintendencia de Industria y Comercio.
A.5.35	Revisión independiente de la seguridad de la información	Si	Se acoge este control dado que para la ANT la revisión periódica e independiente del sistema de gestión de seguridad de la información permite evaluar la conveniencia y eficiencia frente a las necesidades de la Entidad.
A.5.36	Cumplimiento con las políticas, reglas y normas de la seguridad de la información	Si	Se acoge este control dado que la ANT se compromete con el cumplimiento de los requisitos legales y los estándares de seguridad establecidos por el Ministerio de las Tecnologías de la Información y las Comunicaciones a través de la política de Gobierno Digital.
A.5.37	Procedimientos operacionales documentados	Si	Se acoge este control dado que la organización de actividades y flujos de trabajo fomenta y promueve la adopción de oportunidades de mejora en la gestión de seguridad.
A6. Controles Personales			
A.6.1	Revisión de antecedentes	Si	Se acoge el control para revisión de antecedentes de funcionarios y contratistas en las entidades de vigilancia establecidas.
A.6.2	Términos y condiciones de empleo	Si	Se acoge el control para revisión de antecedentes de funcionarios y contratistas en las entidades de vigilancia establecidas.
A.6.3	Concientización, educación y entrenamiento en seguridad de la información	Si	Se acoge el control por medio del Plan Institucional de capacitaciones, eje 4 transformacional digital y cibercultura.
A.6.4	Proceso disciplinario	Si	Se acoge este control dado que para la ANT el incumplimiento de los requisitos del sistema de gestión de seguridad de la información conlleva a exposición a la materialización de riesgos que pueden afectar la misionalidad de la Institución.
A.6.5	Responsabilidades luego de la finalización o cambio de empleo	Si	Se acoge este control ya que para la ANT la desvinculación de funcionarios o contratistas se debe hacer de manera organizada, controlada y rápida para realizar los ajustes pertinentes sobre el acceso a los activos de información, instalaciones de procesamiento de información o equipos informáticos sobre los cuales tuviera acceso el colaborador.
A.6.6	Acuerdos de confidencialidad o no revelación	Si	Se acoge este control ya que es el mecanismo dispuesto por la ANT para que funcionarios, contratistas, proveedores y terceros se comprometan a no divulgar contraseñas u otros mecanismos de autenticación que se les asigne.
A.6.7	Trabajo remoto	Si	Se acoge este control dado que la ANT considera el trabajo remoto como una modalidad de trabajo que se realiza fuera del entorno de las oficinas de la Agencia con gran frecuencia debido al volumen de contratistas y terceros vinculados a la Entidad.
A.6.8	Reportes de eventos de seguridad de la información	Si	Se acoge este control dado que la ANT debe recolectar, analizar y tomar acciones de todos los eventos de seguridad de la información que se puedan presentar en la Entidad.

CONTROL ISO 27K:2022	OBJETIVO DEL CONTROL	APLICA	JUSTIFICACIÓN
A7. Controles Físicos			
A.7.1	Perímetros de seguridad física	Si	Se acoge este control dado que la ANT debe recolectar, analizar y tomar acciones de todos los eventos de seguridad de la información asociados a las instalaciones físicas que se puedan presentar en la Entidad.
A.7.2	Entrada física	Si	Se acoge este control dado que la ANT debe recolectar, analizar y tomar acciones de todos los eventos y registros de seguridad de la información asociados al ingreso físico a las áreas de procesamiento de información de la Entidad.
A.7.3	Seguridad de oficinas, despachos e instalaciones	Si	Se acoge este control dado que la ANT debe recolectar, analizar y tomar acciones de todos los eventos y registros de seguridad de la información asociados al ingreso físico a las áreas de procesamiento de información de la Entidad.
A.7.4	Monitoreo de la seguridad física	Si	Se acoge este control dado que la ANT debe registrar, vigilar y analizar todos los eventos de seguridad de la información asociados a las instalaciones físicas que se puedan presentar en la Entidad.
A.7.5	Protección contra amenazas físicas y ambientales	Si	Se acoge este control dado que la ANT debe prepararse para atender oportuna y eficientemente un evento de desastre natural que afecte los activos de información de la Entidad afectando la disponibilidad de sus servicios.
A.7.6	Trabajo en áreas seguras	Si	Se acoge este control dado que la ANT debe acoger e implementar controles de seguridad en equipo, áreas, aplicaciones y dispositivos de red asociados a la prestación de los servicios estratégicos, misiones y de apoyo ofrecidos por la Entidad.
A.7.7	Escritorio y pantalla limpios	Si	Se acoge este control dado que la ANT debe implementar medidas para que los usuarios dispongan siempre el escritorio y la pantalla libre de accesos rápidos a información confidencial o interna de la Entidad.
A.7.8	Emplazamiento y protección de equipos	Si	Se acoge este control dado que la ANT debe acoger e implementar controles de seguridad en equipo, áreas, aplicaciones y dispositivos de red asociados a la prestación de los servicios estratégicos, misionales y de apoyo ofrecidos por la Entidad.
A.7.9	Seguridad de activos fuera de las instalaciones	Si	Se acoge este control dado que la ANT debe vigilar cualquier dispositivo que sea utilizado fuera de las instalaciones de la Entidad que almacene o procese información de la ANT. Incluye el manejo de dispositivos en la modalidad BYOD (Bring Your Own Device)
A.7.10	Medios de almacenamiento	Si	Se acoge este control dado que la ANT debe implementar una política y controles para la administración de medios de almacenamiento extraíbles y que representan riesgos para la Entidad.
A.7.11	Servicios públicos de apoyo	Si	Se acoge este control dado que la ANT debe prepararse y estar protegida para cortes e interrupción de energía u otros servicios públicos de respaldo en las instalaciones físicas de la Entidad.
A.7.12	Seguridad del cableado	Si	Se acoge este control dado que la ANT debe proteger los cables que transportan energía, datos y voz de eventos de seguridad de la información como interceptación, interferencia o daño.
A.7.13	Mantenimiento de equipos	Si	Se acoge este control dado que la ANT debe comprometerse con garantizar la disponibilidad, integridad y confidencialidad de la información en el cableado de suministro eléctrico y comunicaciones de la Entidad.
A.7.14	Disposición o reutilización segura de equipos	Si	Se acoge este control dado que la ANT debe verificar que los datos confidenciales y el software sin licencia se han eliminado o sobrescrito de forma segura antes de desecharlos o volverlos a usar.
A8. Controles tecnológicos			
A.8.1	Dispositivos de punto final de usuario	Si	Se acoge este control dado que la ANT debe asegurar que los dispositivos de usuario final cuentan con los controles de seguridad requeridos para proteger los activos de información de la ANT.
A.8.2	Derechos de acceso privilegiado	Si	Se acoge este control dado que los accesos privilegiados son limitados y aquellos que por necesidades de la misionalidad de la ANT se requieran conceder deben ser estrictamente monitoreados, controlados y auditados.
A.8.3	Restricción de acceso a la información	Si	Se acoge este control dado que la ANT debe tener claridad y verificar las decisiones sobre el control de acceso a la información gestionada por los procesos de la Agencia.

CONTROL ISO 27K:2022	OBJETIVO DEL CONTROL	APLICA	JUSTIFICACIÓN
A.8.4	Acceso al código fuente	Si	Se acoge este control dado que la ANT debe verificar que el acceso a los códigos fuente de programas y elementos asociados (diseños, especificaciones, planes de pruebas) este restringido únicamente al personal autorizado.
A.8.5	Autenticación segura	Si	Se acoge este control dado que la ANT debe estipular y controlar los mecanismos de seguridad que permiten autenticar a los usuarios de las diferentes cuentas de acceso a sistemas de información y aplicaciones.
A.8.6	Gestión de la capacidad	Si	Se acoge este control dado que la ANT debe ANT debe realizar un seguimiento al uso de los recursos tecnológicos: acceso a redes, almacenamiento, capacidad de procesamiento, disponibilidad de equipos, energía eléctrica, servicios de soporte de centro de datos, suministros para copias de respaldo, licenciamiento de software, y demás componentes de infraestructura de TIC necesarios para la normal prestación de servicios tecnológicos de la Entidad.
A.8.7	Protección contra código malicioso (malware)	Si	Se acoge este control dado que la ANT debe verificar que tanto servidores y estaciones de trabajo cuenten con software especializado para evitar la ejecución de software de código malicioso que potencialmente pueda generar afectaciones a los activos de información de la Agencia.
A.8.8	Gestión de vulnerabilidades técnicas	Si	Se acoge este control dado que la ANT debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información, mediante el monitoreo de listas de interés, información de proveedores, pruebas de técnicas u otras fuentes apropiadas y atender su aplicabilidad en la ANT y oportuna remediación.
A.8.9	Gestión de la configuración	Si	Se acoge este control dado que la ANT debe diseñar, implementar, mantener y mejorar los procedimientos operacionales necesarios para la gestión de los diferentes componentes y servicios de soporte tecnológico.
A.8.10	Eliminación de información	Si	Se acoge este control dado que la ANT debe verificar que los datos confidenciales y el software sin licencia se han eliminado o sobrescrito de forma segura antes de desecharlos o volverlos a usar.
A.8.11	Enmascarado de datos	Si	Se acoge este control dado que la ANT debe garantizar que todas las pruebas requeridas por el desarrollo de software hagan uso de datos enmascarados para evitar revelar la información confidencial de los ambientes de producción.
A.8.12	Prevención de fuga de datos	Si	Se acoge este control dado que la ANT debe aplicar los controles necesarios para prevenir la fuga de datos a través de cualquier medio lógico o físico de la Entidad.
A.8.13	Copia de seguridad de la información	Si	Se acoge este control dado que la ANT debe realizar copias de respaldo de la información institucional, imágenes del software de sistemas operacional activo en los servidores a intervalos regulares y verificar su correcto funcionamiento.
A.8.14	Redundancia de las instalaciones de procesamiento de información	Si	Se acoge este control dado que la ANT debe asegurar la implementación de instalaciones alternas de procesamiento de información que permitan ofrecer disponibilidad y continuidad a los servicios misionales de la Agencia.
A.8.15	Registro	Si	Se acoge este control ya que para la ANT la conservación y protección de registros es relevante para la vigilancia y gestión adecuada de información, activos y accesos que puedan afectar los sistemas de información institucionales.
A.8.16	Actividades de seguimiento	Si	Se acoge este control dado que la ANT debe conservar y revisar regularmente los registros acerca de actividades de los usuarios, excepciones, fallas y eventos de seguridad de la información que afecten a los sistemas de información institucionales.
A.8.17	Sincronización de reloj (clock)	Si	Se acoge este control dado que la ANT debe mantener sincronizados los sistemas y dispositivos con la hora legal colombiana.
A.8.18	Uso de programas de utilidad privilegiados	Si	Se acoge este control dado que la ANT debe restringir el uso de programas utilitarios privilegiados al personal que labore con la ANT dada la capacidad que tiene este tipo de software de eludir los controles de seguridad de los sistemas operativos.
A.8.19	Instalación de software en sistemas operacionales	Si	Se acoge este control dado que la ANT define procedimientos para controlar la instalación de software de sistema operacional en servidores.

CONTROL ISO 27K:2022	OBJETIVO DEL CONTROL	APLICA	JUSTIFICACIÓN
A.8.20	Seguridad en redes	Si	Se acoge este control dado que la ANT debe implementar controles para asegurar la seguridad de la información en las redes y la protección de servicios relacionados contra acceso no autorizado.
A.8.21	Seguridad de servicios de red	Si	Se acoge este control dado que la ANT debe implementar controles para asegurar la seguridad de la información en las redes y la protección de servicios relacionados contra acceso no autorizado.
A.8.22	Segregación de redes	Si	Se acoge este control dado que la ANT debe configurar y mantener la separación de las redes de servicios de información de la ANT en grupos: servicios de información, usuarios y sistemas de información en función de las necesidades de la Entidad.
A.8.23	Filtrado web	Si	Se acoge este control dado que la ANT debe implementar en las redes de acceso a Internet de la ANT políticas de filtrado web y restricción de acceso solo a los sitios web asociados a la prestación de servicios institucionales.
A.8.24	Uso de criptografía	Si	Se acoge este control dado que la ANT debe acoger el uso de controles criptográficos para asegurar la preservación de la confidencialidad de la información pública clasificada y pública reservada.
A.8.25	Ciclo de vida de desarrollo seguro	Si	Se acoge este control dado que la ANT debe velar porque la seguridad de la información sea parte integral de los sistemas de información durante todo el ciclo de vida de desarrollo de software.
A.8.26	Requerimientos de seguridad en aplicaciones	Si	Se acoge este control dado que la ANT debe considerar que todos los requisitos relacionados con seguridad de la información sean incluidos en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
A.8.27	Arquitectura de sistemas seguros y principios de ingeniería	Si	Se acoge este control dado que la ANT debe considerar lineamientos para el desarrollo de software que incluyan principios de ingeniería y controles para garantizar la seguridad de la información durante los procesos de desarrollo de software.
A.8.28	Codificación segura	Si	Se acoge este control dado que la ANT debe asegurar que todos los procesos de desarrollo de software sigan las directrices definidas en el lineamiento de construcción de software definido por la Entidad.
A.8.29	Prueba de seguridad en el desarrollo y aceptación	Si	Se acoge este control dado que la ANT debe asegurar que los procesos de pruebas de seguridad se cumplen en el ciclo de vida del desarrollo del software.
A.8.30	Desarrollo externalizado	Si	Se acoge este control dado que la ANT debe verificar que el desarrollo externalizado cumpla los lineamientos y política Desarrollo de Software formulados por la SSIT.
A.8.31	Separación de entornos de desarrollo, prueba y producción	Si	Se acoge este control dado que la ANT debe verificar que todos los desarrollos de software cuenten con separación de ambientes que eviten problemas en los entornos de producción.
A.8.32	Gestión de cambios	Si	Se acoge este control dado que la ANT debe controlar todos los cambios sobre la infraestructura tecnológica de la ANT.
A.8.33	Información de prueba	Si	Se acoge este control dado que la ANT debe asegurar que todas las pruebas de seguridad requeridas por el desarrollo de software se cumplan junto con las remediaciones necesarias para cerrar brechas de seguridad detectadas.
A.8.34	Protección de sistemas de información durante pruebas de auditoría	Si	Se acoge este control dado que la ANT debe planificar las auditorias y revisiones de terceros de manera organizada y controlada de manera que se mantenga la integridad en los programas y datos.

HISTORIAL DE CAMBIOS		
Fecha	**Versión**	**Descripción**
20/12/2024	1	Primera versión del documento. Esta versión tiene como objetivo documentar y establecer los lineamientos generales del Sistema de Gestión de Seguridad de la Información en la Agencia Nacional de Tierras.

APROBACIÓN				
	NOMBRE	**CARGO**	**FIRMA**	**FECHA**
ELABORÓ	Sandra Liliana Rodríguez Rodríguez	Contratista - Subdirección de Sistemas de Información de Tierras	**ORIGINAL FIRMADO**	20/12/2024
ELABORÓ	Rosa Johanna Rincón Molina	Contratista - Subdirección de Sistemas de Información de Tierras	**ORIGINAL FIRMADO**	20/12/2024
REVISÓ	Andrea Linney Sierra Ladino	Contratista - Subdirección de Sistemas de Información de Tierras	**ORIGINAL FIRMADO**	20/12/2024
APROBÓ	Diana Lucía Herrera Riaño	Subdirectora de Sistemas de Información de Tierras	**ORIGINAL FIRMADO**	20/12/2024

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.