MANUAL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN DE TIERRAS

1. INTRODUCCIÓN

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

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. 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 ISO/IEC 27001.

Ahora bien, en concordancia con estos lineamientos la ANT verifica y actualiza de manera continua el NORMOGRAMA 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.

Es indispensable resaltar en dicha normatividad que la ANT cumple con lo dispuesto en la Ley 1581 de 2012 respecto al tratamiento de datos personales. Considerando el aumento del uso de información digital y el crecimiento exponencial de su empleo con fines comerciales, resulta esencial establecer controles, buenas prácticas y una cultura organizacional orientada a la protección de la privacidad, la prevención del robo de identidad y el resguardo contra fraudes. Asimismo, se busca asegurar que la información se gestione de manera ética y segura. La adecuada protección de datos fortalece la confianza entre empresas y consumidores, además de contribuir a la prevención de delitos informáticos y el uso indebido de datos sensibles.

5. DEFINICIONES

Los términos relacionados a continuación se encuentran relacionados con los aspectos generales de la Seguridad de la información y la ISO/IEC 27001, permiten además la comprensión del presente manual y la articulación de este 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
- **Análisis de impacto al negocio (BIA – Business Impact Analysis):** El proceso de analizar las funciones del negocio y el efecto que una interrupción podría tener sobre ellas
- **ANT:** Agencia Nacional de Tierras
- **Autorización:** Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.
- **Autenticidad:** La entidad que accede al activo de información está verificada y es la que declara ser.
- **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.
- **Crisis:** Una situación anormal, inestable y compleja que amenaza los objetivos estratégicos, la reputación
    - la existencia de una organización.
- **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.
- **Dato sensible:** aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos, los datos relativos a la salud, a la vida sexual, y los datos biométricos.
- **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
- **Información pública clasificada:** de carácter privado o particular que, por ley, no puede ser de acceso público general, se centra más en el ámbito privado de las personas por ejemplo historias clínicas, expedientes pensionales, datos de hojas de vida, información financiera y comercial protegida por ley.
- **Información pública reservada:** por su naturaleza, debe ser restringida temporalmente, protegiendo derechos fundamentales o el interés público, y está sujeta a un periodo de reserva, se enfoca en proteger la seguridad del Estado, derechos fundamentales y secretos comerciales, con una naturaleza más temporal.
- **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.
- **Plan de Continuidad de Negocio (BCP):** Conjunto de procedimientos y acciones que una organización implementa para garantizar que sus funciones esenciales continúen operando durante y después de un evento disruptivo o desastre (como desastres naturales, ciberataques o fallos tecnológicos).

- **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.
- **SoA - Declaración de Aplicabilidad:** Documento dentro de un Sistema de Gestión de Seguridad de la Información (SGSI) que define las políticas, controles de seguridad y medidas que se implementan para cumplir con los requisitos de un estándar o marco de referencia como ISO 27001.
- **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]
- **Trazabilidad:** La actuación sobre un Activo o Información es imputada exclusivamente a la entidad que lo realizó.
- **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.

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*".

La Agencia Nacional de Tierras (ANT), cuenta con una sede principal ubicada en la Cl. 43 #57 41 de la ciudad de Bogotá y una Sede Servicio al Ciudadano en Chapinero en la Cra 13 No. 54-55 Piso 1, Torre SH. Sumado a esto se compone de 32 unidades de Gestión territorial.

En paralelo a ello y según lo establecido en el Plan Estratégico 2023-2026 de la ANT, la Reforma Rural Integral (RRI), incluida en el Acuerdo de Paz de 2016, compromete al Estado Colombiano a impulsar la transformación estructural del campo, garantizando el acceso progresivo de la propiedad rural a quienes lo habitan y en especial a las mujeres.

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.

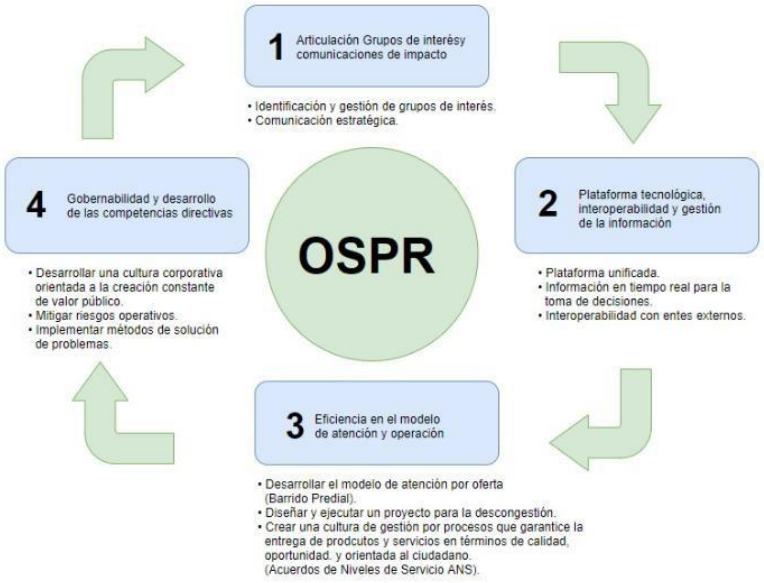
Ahora bien, a través de las actividades de gestión de riesgos y oportunidades y planeación estratégica institucional del proceso de DIRECCIONAMIENTO ESTRATÉGICO (DEST-Caracterización), la Agencia Nacional de Tierras analiza su contexto interno y externo para comprender integralmente su contexto y

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 consolida 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

Tabla 1. Análisis del contexto institucional

ANÁLISIS DEL CONTEXTO INSTITUCIONAL		
CONTEXTO EXTERNO	**POLÍTICOS:** cambios de gobierno, legislación, políticas públicas, regulación.	• Plan Estadístico Sectorial Agropecuario para fortalecer la información estadística sobre la tenencia de la tierra rural • Modelo de datos de administración del territorio definido por el Sistema de Administración del Territorio –SAT-" (Art. 35. Ley 2294 de 2023). • Plan Marco de Implementación formulado por el Gobierno Nacional en el cual se evidencia el compromiso hacia la asignación como el reconocimiento de derechos a los pobladores rurales y comunidades étnicas. • Normativas nuevas que puedan incidir en la operación de la Agencia.
	ECONÓMICOS Y FINANCIEROS: disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.	• Impacto económico causado por la incertidumbre y volatilidades del mercado. • Restricciones presupuestales del Gobierno Nacional que puedan afectar a la ANT.
	SOCIALES Y CULTURALES: demografía, responsabilidad social, orden público.	• Las políticas con Enfoque Diferencial definidas por el Estado que influencian la actuación de la Entidad • Cultura de la informalidad en las comunicaciones y en el uso y transferencia de la información
	TECNOLÓGICOS: avances en tecnología, acceso a sistemas de información externos, gobierno en línea.	• Políticas de Seguridad Digital fortalecida a través de requerimientos de MIPG y norma ISO/IEC 27001 2022 • Avances tecnológicos relacionados con la Inteligencia Artificial. • Disponibilidad de herramientas para el análisis, seguimiento y tratamiento de riesgos en materia de seguridad de la información • Evidencia de una falta de disponibilidad de información actualizada y de detalle por parte de otras entidades nacionales, lo que dificulta que la ANT avance en los procesos de acceso y formalización masiva. • Los frecuentes cambios normativos, en materia de desarrollo rural y de reforma agraria, que implican cambios a nivel tecnológico y de sistemas de información • Plan Nacional de Infraestructura de datos como base para el uso eficaz a nivel público de los mismos. Eventos e incidentes recurrentes de ataques a entidades y empresas relacionados con ciberseguridad.

ANÁLISIS DEL CONTEXTO INSTITUCIONAL		
	AMBIENTALES: emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.	• Situaciones generadas por eventos naturales o antrópicos que pueden afectar las decisiones de la ANT
	LEGALES Y REGLAMENTARIOS: Normatividad externa (leyes, decretos, ordenanzas y acuerdos).	• Las limitaciones, que de tipo legal, existen relacionadas con los usos del suelo rural y que repercuten en los sistemas de información y su parametrización. • Reglamentación y decretos que cambien las condiciones de los procesos y por ende el uso de sistemas de información actuales.
CONTEXTO INTERNO	**FINANCIEROS:** presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.	• Se cuenta con presupuesto para el desarrollo de proyectos de mejora tecnológica y seguridad de la información • Limitación de recursos para tener mayor presencia institucional en las regiones. • Capacidad instalada en la entidad.
	PERSONAL: competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.	• Personal comprometido con el desarrollo de la tarreas y funciones a cargo • Rotación de personal que dificulta la continuidad de procesos y proyectos. • Alta dependencia de contratistas para ejecutar labores relacionadas con TIC.
	PROCESOS: capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.	• Mapa de procesos y procedimientos institucionales bien estructurados • Documentación de procedimientos de seguridad de la información y el tratamiento de riesgos de seguridad de la información • Evidencia de una debilidad en la concientización y generación de una cultura de prevención para la ANT en temas de seguridad de la información, de delitos informáticos y de la custodia de la evidencia digital, lo cual genera dificultades para la investigación forense.
	TECNOLOGÍA: integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.	• Se cuenta con plataformas tecnológicas, ágiles y de fácil acceso, al servicio de los pobladores rurales (FISO) y grupos de interés. • Se implementan procesos para la identificación de las vulnerabilidades técnicas de los sistemas de información de la ANT. • A pesar de contar con las tecnologías no hay unificación de los datos de avances en la gestión institucional entre dependencias. • Escasa coordinación, entre dependencias, para el mejor aprovechamiento de las tecnologías existentes en la Entidad. • Se evidencian debilidades con respecto al uso de algunas plataformas tecnológicas, interoperabilidad y

ANÁLISIS DEL CONTEXTO INSTITUCIONAL		
		gestión de la información, que se están ajustando actualmente. • Insuficiente tecnología informática para el desarrollo, seguimiento y control de proyectos
	ESTRATÉGICOS: direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.	• La ANT cuenta con estructura legal, contexto y actuación a corto, mediano y largo plazo. • Se desarrolla el plan de continuidad del negocios basado en los riesgos de seguridad la información, identificados como críticos. • Actualización de la política de Seguridad y privacidad de la información, como eje base para asegurar la confidencialidad, integridad y disponibilidad de la información de la ANT. • Existe la cultura de revisar y ajustados la documentación de políticas planes, procesos y procedimientos con frecuencia, sin embargo algunos procedimientos requieren revisión, actualización y control de su implementación. • No se evidencia una cultura de calidad enfocada a la integralidad de los sistemas de gestión con los que se cuenta en la entidad y que permita la articulación y gestión eficaz de los mismos, entre dependencias, para el logro de los objetivos de planes, programas y proyectos. • No se evidencia un estado de madurez en relación con el direccionamiento seguro y eficaz de la gestión de la seguridad de la información, sin embargo, se viene consolidando un equipo de trabajo que permite el establecimiento oficial de una línea de control, seguimiento, mitigación y mejora continua.
	COMUNICACIÓN INTERNA: canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.	• Existencia de varios canales informativos y de comunicación internos que se actualizan con frecuencia • Escasa o baja presencia de funcionarios en jornadas de capacitación, como en eventos masivos que se programan referentes a la seguridad de la información. • Se generen nuevas o mucho más ágiles estrategias de comunicación e información, así como la implementación de cronogramas de capacitación que permitan una mayor socialización y sensibilización en temas de seguridad de la información.

Fuente: Elaboración Propia Equipo seguridad de la Información SSIT

6.2. Articulación del MIPG con el Sistema de Gestión de Seguridad de la Información (SGSI)

El Modelo Integrado de Planeación y Gestión (MIPG) y el Sistema de Gestión de Seguridad de la Información (SGSI) mantienen una relación directa y complementaria, orientada al fortalecimiento de la gestión institucional, la protección de la información y la mejora continua de los procesos en las entidades públicas.

En el marco del MIPG, la Dimensión de Control Interno y la Dimensión de Gestión con Valores para Resultados establecen lineamientos para la administración de riesgos, el cumplimiento normativo y la adopción de buenas prácticas de gobierno y gestión. En este contexto, el SGSI se constituye como una herramienta clave para la identificación, análisis, evaluación y tratamiento de los riesgos de seguridad de la información, contribuyendo al logro de los objetivos institucionales y a la protección de los activos de información.

Asimismo, el SGSI apoya la implementación de políticas, procedimientos y controles que fortalecen el ambiente de control**,** la gestión del riesgo**,** las actividades de control y los mecanismos de seguimiento y mejora, elementos fundamentales del MIPG. De esta manera, la seguridad de la información se integra de forma transversal en la planeación, ejecución, seguimiento y evaluación de la gestión institucional.

En conclusión, el SGSI actúa como un componente estratégico que operacionaliza los principios del MIPG en materia de control, gestión del riesgo y mejora continua, asegurando la confidencialidad, integridad y disponibilidad de la información, y contribuyendo al cumplimiento de la misión institucional y a la generación de valor público.

Ahora bien, la articulación del Sistema de Gestión de Seguridad de la Información (SGSI) con el Modelo Integrado de Planeación y Gestión (MIPG) se fundamenta en la adopción de un enfoque integral de gestión, orientado al cumplimiento de los objetivos institucionales, la gestión del riesgo y la mejora continua, conforme a los lineamientos establecidos en la norma ISO/IEC 27001:2022 y la normativa vigente aplicable a las entidades públicas.

Esta articulación permite integrar la seguridad de la información de manera transversal en los procesos estratégicos, misionales, de apoyo y de evaluación de la ANT, asegurando la protección de la confidencialidad, integridad y disponibilidad de la información institucional.

Para tal efecto, se consideran los siguientes elementos, alineados con las cláusulas y principios de la ISO/IEC 27001:2022:

1. Contexto de la organización y alineación estratégica
(Cláusula 4 – Contexto de la organización)

El SGSI se implementa considerando el contexto interno y externo de la entidad, las necesidades y expectativas de las partes interesadas y el alcance definido, en coherencia con la planeación estratégica institucional y los lineamientos del MIPG. La seguridad de la información se integra como un componente habilitador del cumplimiento de los objetivos estratégicos y del direccionamiento institucional.

2. Liderazgo, gobierno y compromiso de la alta dirección
(Cláusula 5 – Liderazgo)

La alta dirección garantiza el liderazgo y compromiso con el SGSI, asegurando su articulación con las dimensiones del MIPG, especialmente la de Direccionamiento Estratégico y Planeación. Se definen roles, responsabilidades y autoridades para la gestión de la seguridad de la información, promoviendo la toma de decisiones informada y el fortalecimiento del gobierno de la información.

3. Planificación y gestión del riesgo de seguridad de la información
(Cláusula 6 – Planificación)

La identificación, análisis, evaluación y tratamiento de los riesgos de seguridad de la información se articulan con el componente de gestión del riesgo del MIPG y el Sistema de Control Interno. Los riesgos del SGSI hacen parte de la gestión de riegos institucional, garantizando coherencia, trazabilidad y priorización, de acuerdo con los criterios de riesgo definidos por la entidad.

4. Soporte y gestión del talento humano
(Cláusula 7 – Soporte)

El SGSI se apoya en la adecuada gestión de los recursos, la competencia, la toma de conciencia y la comunicación, en concordancia con la Dimensión de Talento Humano del MIPG. Se implementan programas de capacitación y sensibilización para fortalecer la cultura de seguridad de la información en todos los niveles de la entidad, acorde con el PIC y con el Plan de cambio, cultura, apropiación, capacitación y sensibilización de Seguridad y Privacidad de la Información y seguridad digital

5. Operación del SGSI y enfoque por procesos
(Cláusula 8 – Operación)

Los controles de seguridad de la información se implementan bajo el enfoque por procesos del MIPG, integrándose de manera transversal en los procesos estratégicos, misionales, de apoyo y de evaluación. Cada proceso identifica y gestiona sus activos de información, riesgos asociados y controles aplicables, conforme al Anexo A de la ISO/IEC 27001:2022.

6. Evaluación del desempeño y control interno
(Cláusula 9 – Evaluación del desempeño)

El desempeño del SGSI se mide, analiza y evalúa mediante indicadores, auditorías internas y revisiones por la dirección, articuladas con la Dimensión de Evaluación de Resultados y el Sistema de Control Interno del MIPG. Esto permite verificar la eficacia de los controles y el cumplimiento de los objetivos de seguridad de la información.

7. Mejora continua del SGSI
(Cláusula 10 – Mejora)

El SGSI se somete a procesos permanentes de mejora continua, en concordancia con el ciclo PHVA promovido por el MIPG y la ISO/IEC 27001:2022. Se gestionan las no conformidades, acciones correctivas y oportunidades de mejora, garantizando la actualización y fortalecimiento del sistema frente a cambios normativos, tecnológicos y organizacionales.

8. Articulación con controles del Anexo A y políticas del MIPG

Los controles definidos en el Anexo A de la ISO/IEC 27001:2022 se implementan de manera coherente con las políticas del MIPG, especialmente las relacionadas con Gobierno Digital, Gestión Documental, Transparencia y Acceso a la Información Pública, Control Interno y Gestión del Conocimiento, asegurando un enfoque integral y complementario de la seguridad de la información.

6.3. 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 y sus necesidades con el objetivo de mantener actualizada la información y dar cumplimiento a los requerimientos de estas en el INTI-F-029 IDENTIFICACIÓN DE NECESIDADES Y EXPECTATIVAS DE GRUPOS DE INTERÉS.

Tabla 2. Grupos de Interés Agencia Nacional de Tierras

Grupo de interés	Necesidades y expectativas
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
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
Ciberdelincuentes	Atacar la infraestructura tecnológica y afectación a bases de datos
Comunidades étnicas	Lograr que la ANT legalice sus territorios
Consejo Directivo - Agencia Nacional de Tierras	Contribuir al cumplimiento del objeto misional de la entidad
Departamento Administrativo de Nacional de Planeación	Garantiza la adecuada formulación y ejecución de los proyectos de inversión
Entidades de control de ciberseguridad (COLCERT, MinTic, entre otras)	Definir políticas y directrices en materia de ciberseguridad.
Entidades del Sector Agrario Adscritas al MADR	Garantizar y coadyuvar la implementación de la política de Desarrollo Rural

Grupo de interés	Necesidades y expectativas
Ministerio de Agricultura y Desarrollo Rural	Rector de la Política Agraria en Colombia
Ministerio de Hacienda y Crédito Público	Garantizar los recursos necesarios para la adecuada formulación y ejecución de los Planes Institucionales
Organizaciones sin ánimo de lucro	Cumplir con la función social que se establece dentro de su objeto misional, apoyando las comunidades étnicas
Rama Judicial - Consejo Superior de la Judicatura	Interponer demandas para que se decida sobre la formalización de la propiedad privada rural.
Superintendencia de Notariado y Registro	Registrar los títulos para la formalización de la propiedad privada rural y los títulos que otorgan
Usuarios	Lograr la legalización y acceso a información. Expectativa que la información se encuentre protegida.

Fuente: *Basado en la información de la Oficina de Planeación – Agencia Nacional de Tierras. Elaboración propia.*

6.4. 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 activos de información de los procesos estratégicos, misionales, de apoyo y de evaluación y control en sus sedes y UGT a nivel nacional.

La Agencia Nacional de Tierras, para el cumplimiento de la misión y el cumplimiento del objetivo, requiere la implementación de lineamientos y medidas de seguridad que permitan asegurar la confidencialidad, integridad y disponibilidad en todo el ciclo de vida de la información, para ello se establece el alcance del Sistema de Gestión de Seguridad de la Información, el compromiso institucional, los límites y las interfaces de la implementación.

Dicho alcance se establece de acuerdo con el cumplimiento de la normatividad legal colombiana vigente y buenas prácticas establecidas en Seguridad de la Información, las cuales se basan en la norma ISO 27001 en su versión 2022 y el Modelo de Seguridad y Privacidad de la Información emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones.

6.4.1. Compromiso Institucional

La Alta Dirección de la Agencia Nacional de Tierras – ANT, en el marco institucional y según los lineamientos exigidos en la Política de Seguridad de la Información y Gobierno Digital, donde se establece la implementación del Sistema de Gestión de Seguridad de la Información – SGSI y del habilitador transversal de seguridad de la información, se compromete a brindar el respaldo humano, financiero y de cualquier índole para el total cumplimiento con lo establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones y los decretos que lo soportan para el cumplimiento normativo y así llegar a estar entre las Entidades del Gobierno Nacional certificadas en Seguridad de la Información.

6.4.2. Límites del SGSI

Con el fin de preservar la confidencialidad, integridad y disponibilidad de la información, el alcance de la implementación del Sistema de Gestión de Seguridad de la Información aplica para todo el personal de planta, contratistas y terceros, los procesos establecidos en la Entidad y los activos de información donde se procesa, almacena y transmite la información, así como los servicios localizaciones y sistemas de información que se describen a continuación:

Procesos

Los procesos que hacen parte de la implementación del Sistema de Gestión de Seguridad de la Información – SGSI son los que se describen a continuación:

- Gestión del modelo de atención
- Planificación del ordenamiento social de la propiedad rural
- Seguridad jurídica sobre la titularidad de la tierra y los territorios
- Acceso a la propiedad de la tierra y los territorios
- Administración de tierras
- Evaluación del impacto del ordenamiento social de la propiedad rural
- Gestión de la información

Con el apoyo de los siguientes procesos:

- Direccionamiento Estratégico.
- Comunicación y gestión con grupos de interés
- Inteligencia de la Información.
- Apoyo Jurídico.
- Gestión del Talento Humano.
- Gestión Financiera.
- Adquisición de bienes y servicios
- Administración de bienes y servicios
- Seguimiento, Medición, Evaluación y Control.

Localizaciones físicas principales

- Oficina Principal ubicada en Calle 43 No.57-41 Bogotá, Colombia.
- Sede Servicio al Ciudadano ubicada en la Carrera 13 No. 54-55 Piso 1, Torre SH, Bogotá, Colombia

Unidades organizativas

- Dirección General.
- Dirección de Gestión del Ordenamiento Social de la Propiedad
- Dirección de Gestión Jurídica de Tierras
- Dirección de Acceso a Tierras
- Dirección de Asuntos Étnicos
- Secretaría General

Áreas de procesamiento

Se compone de las oficinas de cada una de las subdirecciones y demás dependencias de la Agencia relacionadas a continuación:

- Oficina Dirección General
- Sedes de Unidades de Gestión Territorial
- Oficina de Planeación
- Oficina Jurídica
- Oficina del Inspector de la Gestión de Tierras
- Oficina Secretaría General
- Oficina de la Coordinación para la Gestión Contractual
- Oficina de la Subdirección de Talento Humano
- Oficina de la Subdirección Administrativa y Financiera
- Oficina de la Dirección de Gestión del Ordenamiento Social de la Propiedad
- Oficina de la Dirección de Gestión Jurídica de Tierras
- Oficina de la Dirección de Acceso a Tierras
- Oficina de la Dirección de Asuntos Étnicos

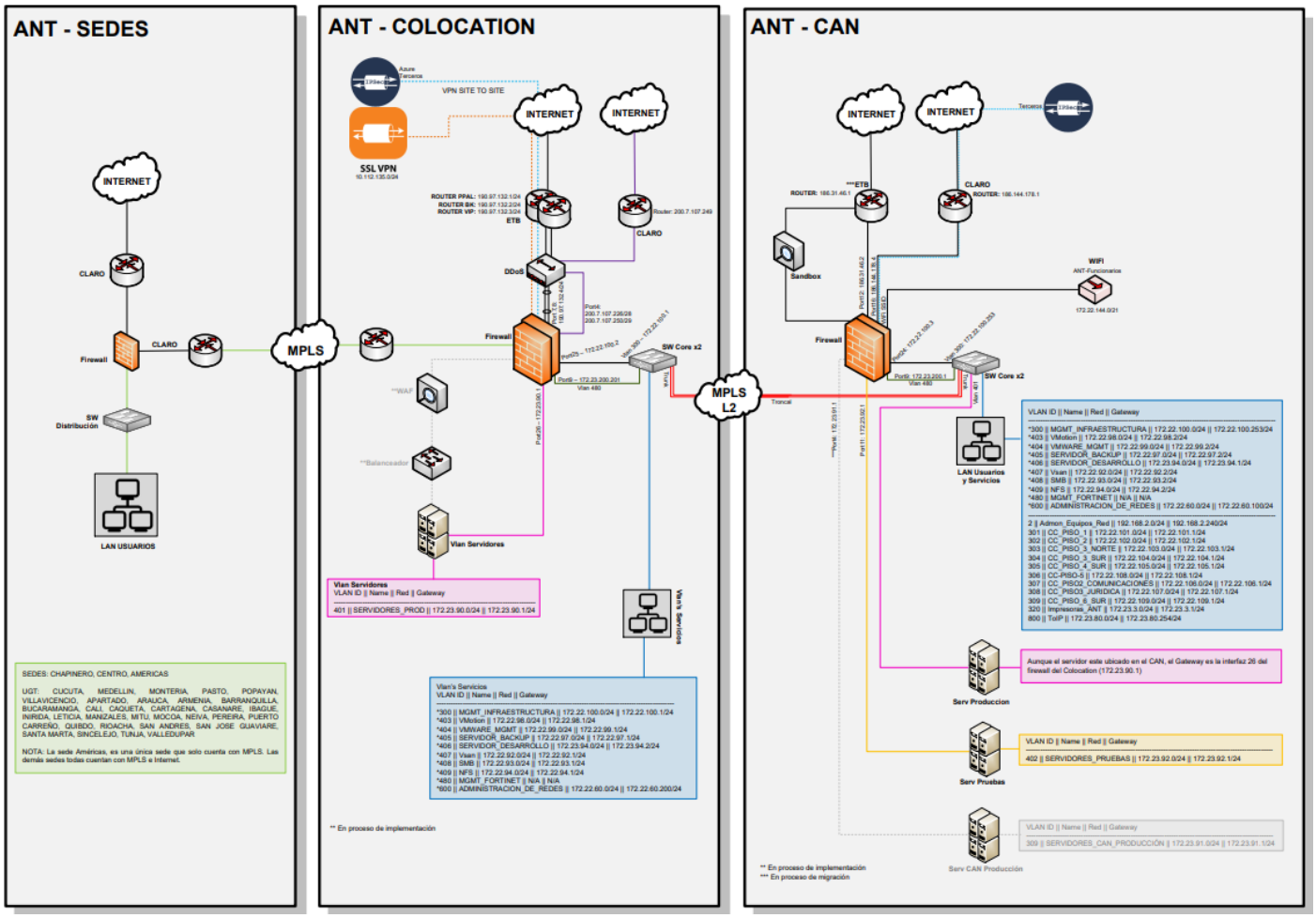
Oficinas de las siguientes Subdirecciones:

- Planeación Operativa
- Sistemas de Información de Tierras
- Seguridad Jurídica
- Procesos Agrarios y Gestión Jurídica
- Acceso a Tierras en Zonas Focalizadas
- Acceso a Tierras por Demanda y Descongestión
- Administración de Tierras de la Nación
- Asuntos Étnicos

Adicionalmente:

- Centro de Datos (Datacenter).
- Centros de Cableado
- Archivo físico sede principal y Chapinero
- Servidores de Archivos Lógicos en la nube para los procesos misionales de la Agencia.

Gráfica 1. Diagrama de red Lógica



Fuente: Equipo de Infraestructura y soporte Tecnológico 2025

Requisitos legales, normativos, contractuales y demás que apliquen

Los requisitos de seguridad de la información se encuentran contemplados en el normograma vigente de la Entidad.

Sistemas de Información / Servicios

Tabla 3. Sistemas de Información Agencia Nacional de tierras

NOMBRE DEL SISTEMA DE INFORMACIÓN	SIGLA	DESCRIPCIÓN
ANT Intranet	Intranet	Portal interno para colaboradores en plataforma SharePoint.
Arcgis Enterprise	Arcgis	Conjunto de productos de software de información geográfica o Sistema de Información Geográfica.
Aula Virtual	MOODLE	Plataforma Moodle donde se desarrollan espacios de formación y capacitación dirigidos a todos los colaboradores de la Agencia.
BALDIOS EDP	EDP	Sistema legado del INCODER que permite la consulta de los procesos de adjudicación para (personas naturales y restitución). Para los procesos de EDP el sistema permite la consulta y gestión de los procesos de adjudicación.
Centro de Atención y Servicios CAS - Aranda	CAS	ARANDA - Mesa de Ayuda - CAS: Permitir registrar y almacenar la información de los usuarios, gestionar solicitudes y realizar un seguimiento de los incidentes, requerimientos, cambios y problemas, asegurando que ninguna solicitud pase desapercibida o quede sin resolver.
CRM	CRM	CRM. Es un Software que facilita a la entidad el proceso de: • Provisión servicio. • Base de conocimiento. • Gestión de casos.
ECARD	ECARD	Es un Software que facilita a la entidad en la carnetización digital.
Field Maps	Field Maps	ArcGIS Field Maps es una aplicación integral que utiliza mapas basados en datos para ayudar al personal a realizar la recopilación y edición de datos móviles, encontrar activos e información, e informar de sus ubicaciones en tiempo real. ArcGIS Field Maps es la aplicación de campo que agiliza los flujos de trabajo críticos que el personal móvil utiliza cada día. Como se integra en ArcGIS, permitirá el uso de los mismos datos a todos los trabajadores, ya se encuentren en campo o en la oficina.
Gestión Solicitudes Sujetos Ordenamiento Territorial Chatbot WhatsApp	Chatbot WhatsApp	Mecanismo de captura y recepción de solitudes RESO.
HEINSOHN SIGEP NÓMINA	HEINSOHN SIGEP	Solución tecnológica diseñada para la liquidación de nómina de entidades públicas que facilita los procesos, seguimientos y evaluaciones de la organización y de las áreas de Talento Humano al interior de la Entidad.

NOMBRE DEL SISTEMA DE INFORMACIÓN	SIGLA	DESCRIPCIÓN
Heródoto	Heródoto	Sistema que permite registrar el seguimiento a los expedientes de los procesos, así como los actos administrativos y planos de formalización asociados a los expedientes gestionados por la Dirección de Asuntos Étnicos, en el marco de los procedimientos relacionados con las comunidades Étnicas. Desde la DAE se está revisando la opción de crear un repositorio con la información que se encuentra en Heródoto con el fin de darle de baja.
KLIC	KLIC	Aplicativo que permite el registro y cargue de los soportes de las actividades gestionadas mensualmente por cada uno de los contratistas, así mismo permite el seguimiento y VoBo de los supervisores de los contratos.
MEGA Hopex	MEGA Hopex	Plataforma de software especializada en Arquitectura Empresarial, utilizada por la ANT para la gestión integrada de los diferentes dominios de arquitectura: Negocio, Datos, Aplicaciones y Tecnología, bajo un enfoque alineado con el marco TOGAF. Funciona como repositorio central de información arquitectónica, permitiendo registrar, relacionar y analizar los elementos que componen el metamodelo institucional, así como consolidar catálogos y establecer las alineaciones internas y externas entre los distintos dominios, facilitando la trazabilidad del modelo arquitectónico de la Entidad.
Módulo de Información Geográfica para el Ordenamiento-MIGO	MIGO	Aplicativo que permite la gestión de información geográfica de la ANT, apoyo transversal al procedimiento único ArcGIS. El MIGO (Módulo de Información Geográfica para el Ordenamiento) es parte integral del Sistema Integrado de Tierras (SIT) de la ANT. Su propósito es consolidar capas de insumos, restricciones y condicionantes para el ordenamiento territorial. La Dirección de Gestión del Ordenamiento Social de la Propiedad se encarga de su conformación, mientras que la Subdirección de Sistemas de Información de Tierras administra el sistema y publica sus capas de información. MIGO es fundamental para los Informes Técnicos Jurídicos en el Procedimiento Único.
ORFEO	ORFEO	Aplicativo de gestión documental que permite gestionar la correspondencia interna, entrante y saliente según la TRD definida. Adicionalmente permite gestionar de los expedientes creados desde el SIT.
Portal Web Agencia Nacional de Tierras	Portal Web	Gestor de contenidos para el portal web.

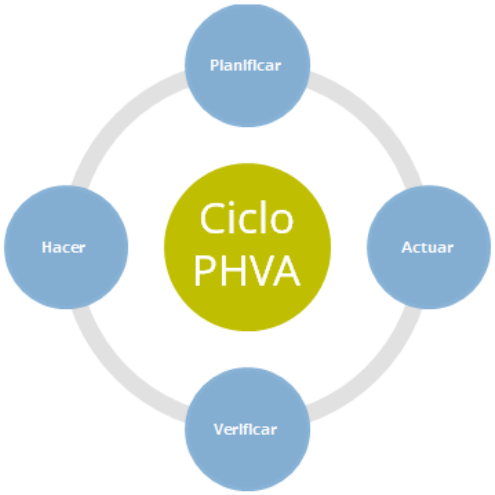
NOMBRE DEL SISTEMA DE INFORMACIÓN	SIGLA	DESCRIPCIÓN
Registro de Sujetos de Ordenamiento RESO - Orquestador	RESO - Orquestador	Herramienta técnica administrada por la subdirección de sistemas de información de tierras de la Agencia Nacional de Tierras para consignar públicamente a todos los individuos y comunidades cuyas relaciones con la tierra deban ser resueltas, tramitadas o gestionadas por la ANT. Aplicativo central responsabilizado de la recepción, persistencia, procesamiento y documentación de solicitudes a través de la coordinación de 4 bases de datos, 9 microservicios y más de 30 endpoints. Permite validar, incluir y Calificar de manera automatizada a los sujetos de ordenamiento territorial, herramienta de entrada a sujetos de ordenamiento a los procesos de la agencia.
Sistema de Alertas y Respuestas Tempranas-SART	SART	Es una plataforma denominada SART (Sistema de Alerta y Respuesta Tempranas) que hace parte del módulo del SIT (Sistema Integrado de Tierras) de la ANT, permitirá el registro y seguimiento a los conflictos identificados por el equipo de dialogo social. Sistema embebido en SIT.
Sistema de Gestión de Expedientes-SIGE	SIGE	Sistema de la Subdirección en el cual se tiene el universo de expedientes del procedimiento de adjudicación de baldíos persona natural y en el cual se registra toda la información de productos emitidos en relación a un expediente por parte de los grupos misionales de la SATDD y de las Unidades de Gestión Territorial, además el cual funciona como insumo para todo tipo de reportes solicitados a esta dependencia.
Sistema Integrado de Barridos-SIB	SIB	Sistema que permite recopilar, organizar, administrar, analizar, compartir y distribuir la información alfanumérica y geográfica generada.
Sistema de Información Geográfico SIG-Formalización	SIG-Formalización	SIG - Sistemas de Formalización MARD heredado a la Subdirección de Sistemas de Información donde deposita las solicitudes de rezago por vía administrativa, notarial y judicial para su respectivo tramite. Si bien fue un aplicativo dado por el Ministerio de Agricultura y en su momento la responsabilidad y desarrollo estaba en la Subdirección de Seguridad Jurídica ahora no se cuenta con soporte ni desarrollo en dicho aplicativo y la base de datos está en los servidores de la ANT.
Sistema Integrado de Tierras-SIT	SIT	Sistema de información, que permite gestionar y procesar de manera articulada y centralizada la información que se genera en la Agencia. Está compuesto por una serie de módulos que soportan aquellos procesos misionales de la ANT, como así mismo aquellos que son transversales.
Sistema Integral Directo de Reforma Agraria-SIDRA	SIDRA	Subsidio Integral Directo de Reforma Agraria. Sistema que permite documentar y validar las actividades para el otorgamiento del subsidio a los potenciales beneficiarios priorizados en el marco de lo establecido en el acuerdo 310 del 2013. Sistema Embebido en SIT.
Survey123	Survey123	ArcGIS Survey123 es una solución completa centrada en formularios para crear, compartir y analizar encuestas. Usado para crear formularios inteligentes con lógica de omisión, valores predeterminados y compatibilidad con varios idiomas. Adicionalmente, puede recopilar datos a través de la web o dispositivos móviles,

NOMBRE DEL SISTEMA DE INFORMACIÓN	SIGLA	DESCRIPCIÓN
		incluso cuando esté desconectado de Internet. Analiza los resultados rápidamente y carga datos de forma segura para su posterior análisis.

Fuente: *Subdirección de Sistemas de Información de tierras 2025*

6.5. 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, este se desarrolla mediante la implementación de un ciclo PHVA que establece las siguientes etapas:



a) Planificar

En esta etapa se debe definir el alcance del Sistema de Gestión de Seguridad de la Información según la norma ISO27001, es decir, especificar y definir los términos de negocio de la Entidad, la organización, la localización de ésta, los activos y la tecnología con la que cuenta, además, de establecer la necesaria justificación de cualquier exclusión.

b) Hacer

En esta etapa es importante definir un plan de tratamiento de riesgos en el que se identifiquen los

recursos, acciones, responsabilidades y prioridades durante la gestión de riesgos en el Sistema de Gestión de Seguridad de la Información.

c) Verificar

La Entidad tiene que efectuar los procedimientos de monitorización y revisión para detectar a tiempo todos los errores generados en los resultados obtenidos en el procesamiento de la información. Debe identificar los incidentes de seguridad y ayudar a la Dirección de la Entidad a determinar si las actividades desarrolladas por las personas y los dispositivos tecnológicos ayudan a garantizar la seguridad de la información.

d) Actuar

La Entidad deberá, de forma periódica, implementar en el Sistema de Gestión de Seguridad de la Información todas las mejoras identificadas, realizar las acciones preventivas y correctivas que sean necesarias en relación con lo que disponga la norma ISO 27001.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/IEC 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, la misma es aprobada por el Comité Institucional de Gestión y Desempeño, y en esta 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, en este sentido y teniendo en cuenta que la actualización del Sistema de Gestión de Seguridad de la Información es dinámica se deben documentar las acciones realizadas en el marco de este y por lo menos una vez al año se deben presentar, los avances o cambios realizados, en el Comité de Seguridad que hace parte del Comité Institucional de Gestión y Desempeño (CIGD) o el que haga sus veces, lo que implica que es a través de este comité que se da la aprobación de la documentación relacionada con Seguridad de la información.

Se debe tener en cuenta que 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, con la salvedad que en el CIGD solo se presentaran para revisión y aprobación las Políticas y Lineamientos relacionados con seguridad de la información, los demás documentos podrán ser actualizados, revisados y aprobados desde la Subdirección de Sistemas de Información de Tierras.

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 que se describe en este Manual, con el objetivo de mantener el ciclo de mejora continua al que responde el SGSI en línea con el Modelo de Seguridad y Privacidad de la Información de la Entidad.

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.	·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

ROL	RESPONSABILIDADES	AUTORIDAD
	·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	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

ROL	RESPONSABILIDADES	AUTORIDAD
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 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	• 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
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

ROL	RESPONSABILIDADES	AUTORIDAD
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. ·Informar sobre el cumplimiento de las directrices de Seguridad de la Información en el marco de la	Requerir información sobre los soportes de implementación de los controles de SGSI

ROL	RESPONSABILIDADES	AUTORIDAD
	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	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

ROL	RESPONSABILIDADES	AUTORIDAD
	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.	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 ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 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/IEC 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. Objetivos e Indicadores 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. **(Indicador: controles implementados/Controles a implementar)**

- 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. **(Indicador: Actividades del plan de sensibilización ejecutadas /actividades incluidas en el plan de sensibilización).**

- Gestionar las situaciones (incidentes y eventos) de seguridad de la información. **(Indicador: situaciones atendidas/situaciones reportadas o detectadas).**

- 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. **(Indicador: eventos gestionados por las herramientas de ciberseguridad/eventos de detectados por las herramientas de ciberseguridad).**

- 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**. (Indicador: Resultado del autodiagnóstico del 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 Y SEGURIDAD 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 Y SEGURIDAD DE LA INFORMACIÓN y teniendo en cuenta la aceptabilidad de los roles y responsabilidades establecidos para el SGSI.

Desde el proceso de INTELIGENCIA Y SEGURIDAD 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, esto mediante la implementación del Plan de cambio, cultura, apropiación, capacitación y sensibilización de Seguridad y Privacidad de la Información y seguridad digital, el cual está alineado al PIC de la Entidad.

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/IEC 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 y cumplen con los procedimientos y lineamientos establecidos en el PLAN DE COMUNICACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

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 ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 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 y asignados para seguridad de la Información.

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

La Declaración de Aplicabilidad (SoA) tiene como propósito identificar, justificar y documentar los controles seleccionados para el Sistema de Gestión de Seguridad de la Información (SGSI) de la organización. Este documento establece el conjunto de controles definidos en la norma aplicable y determina cuáles de ellos son implementados, excluidos o gestionados mediante otros mecanismos, en función del análisis de riesgos y de los requisitos legales, contractuales y organizacionales.

La SoA constituye un componente esencial del SGSI, ya que proporciona una visión transparente y estructurada del nivel de protección adoptado por la organización. Asimismo, sirve como referencia para auditorías internas y externas, facilitando la verificación del cumplimiento y la eficacia de los controles seleccionados, para la ANT la información de la misma se registra en el INTI-F-030 DECLARACIÓN DE APLICABILIDAD (SoA Statement of Applicability).

HISTORIAL DE CAMBIOS		
Fecha	**Versión**	**Descripción**
20/12/2024	01	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.
18/12/2025	02	Actualización del documento mediante la articulación del mismo con los cambios y actualizaciones del MSPI versión 2025. ▪ Ampliación y fortalecimiento del contexto, alcance y partes interesadas ▪ Especificación para la revisión y aprobación de documentos relacionados con seguridad de la información ▪ Inclusión y formalización de formatos anexos, para la identificación de necesidades de grupos de interés y Declaración de aplicabilidad ▪ Articulación del documento con el MIPG ▪ Inclusión de los indicadores de Seguridad de la Información.

APROBACIÓN				
	NOMBRE	**CARGO**	**FIRMA**	**FECHA**
ELABORÓ	Juan Carlos Lobo Torres	Contratista Subdirección de Sistemas Información de Tierras	**ORIGINAL FIRMADO**	10/12/2025
ELABORÓ	Rosa Johanna Rincon Molina	Contratista Subdirección de Sistemas Información de Tierras	**ORIGINAL FIRMADO**	10/12/2025
REVISÓ	Diana Lucía Herrera Riaño	Subdirectora Sistemas de Información de Tierras	**ORIGINAL FIRMADO**	15/12/2025
APROBÓ	**APROBACIÓN Y PUBLICACIÓN DEL MANUAL** 4ª Sesión Comité Institucional de Gestión y Desempeño del 18/12/2025			18/12/2025