PLAN DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025

DIRECCIÓN DE GESTION DEL ORDENAMIENTO SOCIAL DE LA PROPIEDAD

SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN DE TIERRAS

CONTENIDO

1. INTRODUCCIÓN 3
2. DEFINICIONES 4
3. OBJETIVOS 7
   3.1. Objetivo general 7
   3.2. Objetivos específicos 8
4. ALCANCE 8
5. BASE LEGAL 8
6. RECURSOS. 10
7. RESPONSABLES 10
8. METODOLOGÍA IMPLEMENTACIÓN MODELO DE SEGURIDAD 13
   8.1. Fase I (Diagnóstico) 14
   8.1.1. SITUACIÓN ACTUAL DE LA ANT 14
   8.2. Fase II Implementación Plan de Seguridad y Privacidad de la Información 19

1. INTRODUCCIÓN

La Agencia Nacional de Tierra ha definido la información como uno de sus activos más valiosos, lo que hace que dentro del plan de gestión de seguridad y privacidad de la información se promueva la conservación de los principios de la seguridad de la información como son la integridad, disponibilidad y confidencialidad por medio de una gestión planificada y eficiente.

Como toda organización se debe ser consciente que las amenazas actuales en temas tecnológicos atentan gravemente contra la seguridad y privacidad de la información, lo que hace que representen un riesgoque al materializarse puede afectar seriamente a la entidad con altos costos económicos, imposición de sanciones legales,afectación de su buena imagen, la continuidad de la operación y del negocio, la desestabilización del CORE por la pérdida de la información entre otras situaciones.

En la medida que las entidades tengan una visión general de los riesgos que pueden afectar la seguridad y privacidad de la información, podrán establecer controles y medidas eficientes, efectivas y transversales con el propósito de salvaguardar la disponibilidad, integridad y confidencialidad de la información y que garantizan la continuidad del negocio, por lo anterior es importante resaltar la necesidad de que las organizaciones realicen una adecuada identificación, clasificación y valoración de los riegos que pueden afectar la seguridad de la información, con el propósito de implementar medidas y controles efectivos que les permitan estar preparados ante situaciones adversas que puedan comprometer los sistemas de información, la infraestructura de TI, el recurso humano, la seguridad física y lógica.

La ANT como máxima autoridad de las tierras de la Nación, es responsable de garantizar debidamente la gestión de su información, razón por la cual debe establecer un marco normativo de un Sistema de Gestión Seguridad de la Información – SGSI que apalanque las políticas, lineamientos, planes, procedimientos, responsabilidades y obligaciones sobre seguridad de la información en el entorno organizacional, es por ello que el presente documento contiene el plan de gestión de la seguridad y privacidad de la información como base para la creación del SGSI de la ANT y la Política de Gobierno Digital, adoptándose como referencia el Modelo de Seguridad y Privacidad de la Información, así como la norma ISO 27001[1] que proporciona un marco metodológico basado en buenas prácticas sobre seguridad de la información.

[1] https://www.normas-iso.com/iso-27001/

2. DEFINICIONES

• Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

• Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

• Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

• Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

• Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

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

• Causa: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

• Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

• Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

• Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada. Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son

puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

• Disponibilidad: Propiedad que la información sea accesible y utilizable por solicitud de los autorizados (2.10 ISO 27000).

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

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

• Evitación del riesgo: Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.
• Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

• Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

• Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

• Identificación del riesgo. Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

• Impacto. Cambio adverso en el nivel de los objetivos del negocio logrados.

• Integridad: Propiedad de salvaguardar la exactitud y el estado completo de los activos (2.36 ISO 27000). Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

• Información: Conjunto de datos que tienen un significado.

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

• Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

• Monitoreo: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de con trol o las diferentes auditorías de los sistemas integrados de gestión.

• Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

• Parte interesada: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

• Probabilidad: Posibilidad de que una amenaza se materialice.

• Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

• Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado.

• Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

• Reducción del riesgo. Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

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

• Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

• Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles. Riesgo Positivo: Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.

• Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

• Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera.

• Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

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

• Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

• Tratamiento del Riesgo: Proceso para modificar el riesgo" (Icontec Internacional, 2011).

• Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

• Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

3. OBJETIVOS

3.1. Objetivo general

Actualizar el Plan de Gestión de Seguridad y Privacidad de la Información mediante una serie de acciones que apoyen la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en la Agencia Nacional de Tierras, teniendo en cuenta los requerimientos y actividades contempladas en el Modelo de Seguridad y Privacidad de la Información MSPI de la estrategia de Gobierno Digital, los objetivos misionales de la ANT, y el cumplimiento a las disposiciones legales vigentes nacionales e internacionales.

3.2. Objetivos específicos

- Optimizar la gestión de la seguridad de la información al interior de la ANT.
- Contribuir en la implementación del Sistema de Gestión de Seguridad de la Información de la ANT de acuerdo con los requerimientos establecidos en el MSPI de la estrategia de Gobierno Digital.
- Establecer lineamientos para la implementación y/o adopción de mejores prácticas de seguridad en la ANT.

4. ALCANCE

El presente plan de gestión aplica para los procesos estratégicos de la Agencia Nacional de Tierras, con el fin de dar cumplimiento a la implementación de la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información basado en la NTC/IEC ISO 27001:2013 y la Política de Seguridad Digital.

5. BASE LEGAL

- Constitución Política de Colombia. Artículos 15, 20, 23 y 74.
- Modelo de Seguridad y Privacidad de la Información MINTIC
- Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- • Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Ley 1341 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones - TIC- Se crea la agencia Nacional de espectro y se dictan otras disposiciones.
- Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

- Ley 527 de 1999. Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- Decreto 338 de 2022. Por el cual se adiciona el Titulo 21 a la parte 2 del libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.
- Decreto 767 de 2022. Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1008 del 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 612 de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado", donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.
- Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 2364 de 2012. Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
- Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- Resolución 0448 de 2022. Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se deroga la resolución 2256 de 2020.

- Resolución 746 de 2022. Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021
- Resolución 500 de 2021. Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital
- Resolución 1519 de 2020. Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
- Resolución 924 de 2020. Por la cual se actualiza la Política de Tratamiento de Datos Personales del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones y se deroga la Resolución 2007 de 2018.
- CONPES 3995 de 2020. Confianza y Seguridad Digital.
- CONPES 3854 de 2017. Política Nacional de Seguridad digital
- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- Directiva 26 de 2020. Diligenciamiento de la información en el índice de transparencia y acceso a la información – ITA – de conformidad con las disposiciones el artículo 23 de la ley 1712 de 2014.

6. RECURSOS.

- ESTRATÉGICOS: Documentación asociada a Políticas, lineamientos, procedimientos y planes de seguridad de la ANT.

- HUMANOS: La Subdirección de Sistemas de Información es responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Entidad en lo concerniente a la seguridad y privacidad de la información lo cual contribuye a la mejora continua, la Dirección de Gestión del Ordenamiento Social de la Propiedad, la Secretaría General, la Subdirección de Talento Humano, los líderes de los procesos y la Oficina de Control Interno, apoyaran operativa y técnicamente en la atención y supervisión necesaria según el rol designado.

- SOTWARE: Equipos virtualizados, herramientas y software para la seguridad de TI.

- FÍSICOS: Infraestructura de TI, redes, comunicaciones y controles de acceso físico.

7. RESPONSABLES

La responsabilidad de las actuaciones en temas de seguridad está enmarcada en:

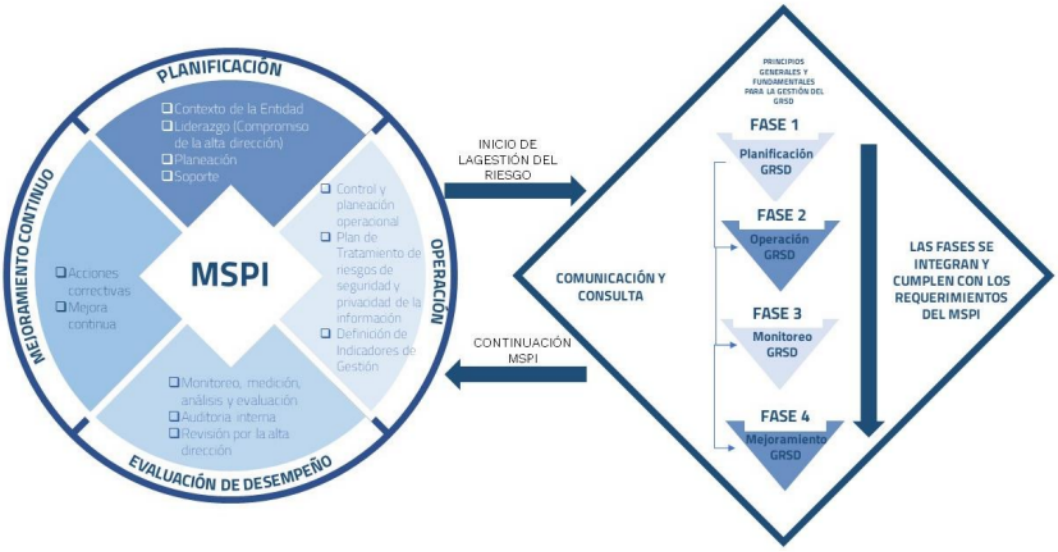
ROL	RESPONSABILIDADES	AUTORIDAD
Alta Dirección	•Aprobación de los alcances, políticas, lineamientos, normas, directrices y procedimientos, así como herramientas, manuales, modelos de operación, metodologías y estructuras organizacionales empleadas para la gestión del MSPI y seguimiento a su cumplimiento 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 evaluación de impacto relativa a la protección de datos. • Atender los lineamientos y requerimientos que le haga 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
	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

ROL	RESPONSABILIDADES	AUTORIDAD
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 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.	Requerir información sobre los soportes de implementación de los controles de SGSI
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. METODOLOGÍA IMPLEMENTACIÓN MODELO DE SEGURIDAD

Ilustración 1 Ciclo del Modelo de Seguridad y Privacidad de la Información



Fuente: MinTIC. Anexo 1 Modelo de Seguridad y Privacidad MSPI, (2021).

8.1. Fase I (Diagnóstico)

Objetivo: Identificar el estado de la ANT con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información - MSPI.

Esta fase permite identificar el estado actual de la ANT (Análisis GAP) con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información, el resultado de este diagnóstico sirve para dar inicio al MSPI.

8.1.1. SITUACIÓN ACTUAL DE LA ANT

A continuación, se presenta el autodiagnóstico del Modelo de Seguridad y Privacidad de la Información como parte de la Política Nacional de Gobierno Digital, basada en la ISO/EC 27001:2013:

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	60	100	EFECTIVO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	31	100	REPETIBLE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	60	100	EFECTIVO
A.8	GESTIÓN DE ACTIVOS	29	100	REPETIBLE
A.9	CONTROL DE ACCESO	49	100	EFECTIVO
A.10	CRIPTOGRAFÍA	40	100	REPETIBLE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	42	100	EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	50	100	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	54	100	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	45	100	EFECTIVO
A.15	RELACIONES CON LOS PROVEEDORES	30	100	REPETIBLE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	23	100	REPETIBLE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	27	100	REPETIBLE
A.18	CUMPLIMIENTO	31	100	REPETIBLE
PROMEDIO EVALUACIÓN DE CONTROLES		**41**	**100**	EFECTIVO

Tabla 1. Resultados de evaluación de efectividad de controles.

Fuente: Modelo de Seguridad y Privacidad de la Información – MSPI ANT Portada.

Los resultados de la evaluación del estado actual de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) revelan una situación dual. Por un lado, se evidencia avances en la planificación, considerando que partimos de una base inicial escasa. Sin embargo, las etapas posteriores de evaluación de desempeño y mejora continua presentan un avance inferior al esperado. Es necesario intensificar los esfuerzos en estas etapas y realizar seguimientos periódicos para desarrollar e implementar los controles y las recomendaciones necesarias para asegurar la optimización del modelo y alcanzar los resultados deseados.

En el resumen de la evaluación de efectividad de controles del instrumento Modelo de Seguridad y Privacidad de la Información (MSPI) de la Agencia Nacional de Tierras (ANT), tiene como objetivo medir la efectividad de los controles de seguridad implementados, donde se refleja:

- **Dominios Efectivos** (lograron una calificación mayor o igual a 40 puntos), equivalente a un 50% del total de dominios:
    - Políticas de seguridad de la información
    - Seguridad de los recursos humanos
    - Control de acceso
    - Seguridad física y del entorno
    - Seguridad de las operaciones
    - Seguridad de las comunicaciones
    - Adquisición, desarrollo y mantenimiento de sistemas

- **Dominios Repetibles** (lograron una calificación menor a 40 puntos), equivalente a un 50% del total de dominios:
    - Organización de la seguridad de la información
    - Gestión de activos
    - Criptografía
    - Relaciones con los proveedores
    - Gestión de incidentes de seguridad de la información
    - Aspectos de seguridad de la información de la gestión de la continuidad del negocio
    - Cumplimiento

Con lo anterior se identifica el nivel de madurez actual de los controles de seguridad, donde se identifican las brechas y áreas de mejora, a partir de los cuales se pueden definir las acciones correctivas necesarias para alcanzar un nivel de protección óptimo

Ahora bien, el gráfico de araña presenta una visión integral del estado de los controles de seguridad, destacando tanto los puntos fuertes como las áreas de mejora. Se observa una calificación "EFECTIVA" (mayor o igual a 40 puntos) en dominios como políticas de seguridad y seguridad de los recursos humanos. No obstante, es necesario establecer acciones de mejora en áreas como:

- La gestión de incidentes
- El cumplimiento
- La relación con proveedores
- La seguridad en la gestión de la continuidad del negocio
- La adquisición de sistemas

Las cuales obtienen una calificación "REPETIBLE" (menor a 40 puntos), lo que ha permitido establecer un plan de cierres de brechas para lograr en estos aspectos una calificación "EFECTIVA" en la siguiente evaluación.

Gráfico 1. Brecha anexo ISO27001:2013.
Fuente: Modelo de Seguridad y Privacidad de la Información – MSPI ANT Portada

Cada una de las acciones desarrolladas permite el alcance del Plan de Seguridad y privacidad de la Información durante el año 2024 en un 100%, porcentaje que permitió el desarrollo de acciones entre las que se desatacan:

- Actualización del BCP (Plan de Continuidad del Negocio)
- Actualización del DRP (Plan de Recuperación ante Desastres)
- Implementación de NOC (**Centro de Operaciones de Red**),
- Implementación del SOC (**Centro de Operaciones de Seguridad**)
- Implementación del SIEM (**Gestión de información y eventos de seguridad**)
- Construcción de un Plan de Cierres de Brechas que permita la mejora continua y el alcance de los objetivos de la entidad de manera progresiva.
- Creación del Manual del Sistema de Gestión de Seguridad de la Información
- Actualización de 9 documentos relacionados con Seguridad de la Información.
- Desarrollo del Plan de capacitación y socialización sobre conceptos y procedimientos de Seguridad de la Información

Actividad	Producto/entregable	ALCANCE 2024
Creación e Implementación Sistema de Gestión de Seguridad de la Información – SGSI	Sistema de Gestión de Seguridad de la Información – SGSI	100%
Políticas de Seguridad de la Información: Se deben revisar, ajustar, actualizar, documentar y socializar periódicamente las Política de Seguridad de la Información, lineamientos, planes, procedimientos específicos de seguridad de la información alineadas con lo definido por MinTIC y por lo exigido en la norma ISO 27001:2013, estas políticas se deben aprobar por la Alta Dirección y divulgadas a todos los interesados.	Políticas de Seguridad de la Información	100%
Activos de Seguridad de la Información: Se debe realizar la identificación y valoración de los activos de información de todos los procesos, haciendo énfasis en los de tipo información, por la criticidad y sensibilidad de esta en la ANT. • Consolidado inventario activos de información • Registro de activos de información • Índice de clasificación y reserva de los activos de información	Registro de Activos de Seguridad de la Información	100%
Articulación en mesas de trabajo para revisión de la matriz actualizada con los líderes de TI (AE, BPM, BD RESO, Aplicaciones, EIST)	Registros de asistencia mesas técnicas	100%
Construir los lineamientos de aseguramiento de credenciales para el acceso a los recursos compartidos y sistemas de información	Lineamiento de Acceso a la Información	100%
Protege la red LAN y DMZ de las amenazas externas que constantemente se encuentran en Internet, además, con el fin de mejorar el nivel de seguridad, se deben adquirir herramientas o software adicional para garantizar la seguridad perimetral.	Herramienta de software para protección en la seguridad perimetral	100%
Implementar esquemas de cifrado para los equipos móviles, unidades de almacenamiento externo o portátiles, para la información que es transportada o que es compartida con terceros, así mismo, se debe adquirir una solución de cifrado que permita compartir o transportar la información de manera segura.	Implementación del esquema de cifrado para la Transferencia Segura de la Información	100%
Generar una herramienta que permita documentar el proceso monitoreo de seguridad.	Herramienta de software para el monitoreo de eventos de seguridad	100%
Realizar pruebas de Ethical Hacking en la plataforma tecnológica permitiendo que sus resultados ayuden a blindar de la mejor manera la información y los servicios de red. Para garantizar el servicio web sobre HTTPS.	Pruebas de Ethical Hacking	100%
Realizar la gestión de la seguridad, que abarca la consideración de los requisitos de seguridad desde el inicio del proyecto, la inclusión de cláusulas de seguridad pertinentes y la exigencia de estándares de seguridad al adquirir equipos o soluciones.	Plan de Acción de Seguridad	100%
Realizar planes de tratamiento de las vulnerabilidades identificadas, dándole prioridad a las críticas altas, continuar con las medias y bajas	Plan de tratamiento de las vulnerabilidades	100%

Actividad	Producto/entregable	ALCANCE 2024
Realizar un Bussines Impact Analisys (BIA) o Análisis de Impacto al Negocio para poder determinar el Punto Objetivo de recuperación (RPO - Recovery Point Objetive), el Tiempo Objetivo de recuperación (RTO - Recovery Time Objetive) y demás variables importantes que respondan a las necesidades de disponibilidad de los servicios TI de la ANT, para proponer adelantar un proyecto de Plan de Continuidad del Negocio que comprende aspectos más amplios de la continuidad. Entregables: • BCP • DRP	Análisis de Impacto al Negocio (BIA), Punto Objetivo de Recuperación (RPO) y Tiempo Objetivo de Recuperación (RTO), se articulan entre sí para formar el Plan de Recuperación de Desastres (DRP)	100%
Realizar campañas de sensibilización en temas de seguridad de la información.	Campaña de sensibilización en materia de seguridad de la información.	100%
Realizar de manera periódica capacitaciones de privacidad de protección de datos personales, así mismo, se debe realizar auditorías que permitan establecer el cumplimiento de la ley.	Capacitaciones de sensibilización en materia de seguridad de la información.	100%

8.2. Fase II Implementación Plan de Seguridad y Privacidad de la Información

GESTIÓN	ACTIVIDADES
Activos de Información	Actualización del instructivo para la valoración de activos de información de acuerdo a la herramienta diseñada
	Actualización Matriz de Activos de Información con su respectiva valoración, mediante el desarrollo de mesas técnicas
	Publicación de Activos de Información
	Registros activos de información ley 1712
Gestión de Riesgos	Revisión y actualización del procedimiento para administración de riesgos de seguridad de la información
	Identificación de Riesgos de Seguridad y Privacidad de la Información
	Aceptación de Riesgos Identificados
	Establecimiento de acciones preventivas - Aceptación perfiles de riesgo
	Consolidación, aprobación y publicación del mapa de riesgos
Revisión de los controles de la norma ISO 27001	Ejercicios trimestrales de inspecciones a controles de acuerdo con SoA
	Seguimiento a hallazgos detectados en las inspecciones
Gestión de Incidentes de Seguridad y Privacidad de la Información	Publicar y Socializar el procedimiento actualizado de incidentes de seguridad de la información

GESTIÓN	ACTIVIDADES
	Gestionar los incidentes y/o ataques de Seguridad de la Información identificados
	CSIRT - Socializar los boletines informativos de seguridad, Integrar con CSIRT de Gobierno
Vulnerabilidades	Definir mecanismos para el Análisis de Vulnerabilidades
	Apoyar en la ejecución de las pruebas de vulnerabilidades
	Seguimiento al plan de remediación de acuerdo con las vulnerabilidades identificadas
Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Elaborar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación
	Ejecutar del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación
	Reporte trimestral de gestión del Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación
Matriz de verificación de Requisitos Legales de Seguridad de la Información	Actualizar la Matriz de verificación de Requisitos legales de Seguridad de la Información
	Establecer acciones que dan cumplimiento a los Requisitos legales de Seguridad de la Información en la entidad
	Publicar y Socializar la Matriz de verificación de Requisitos legales de Seguridad de la Información
Plan de Continuidad del Negocio	Actualización del Análisis de Impacto de la operación 2025
	Seguimiento de Riesgos de Interrupción
	Actualización de Documentación de Estrategias de Continuidad
	Seguimiento Implementación Estrategias de Continuidad
	Documentación del Plan de continuidad de la Operación actualizado 2025
Gobierno Digital	Actualizar el documento de autodiagnóstico de la entidad en la implementación de Seguridad y Privacidad de la Información
	Revisar y alinear la documentación del SGSI de la entidad al MSPI, de acuerdo con la Normatividad vigente.
	Realizar el análisis de brechas en la implementación de controles de seguridad física por parte de los colaboradores de la entidad
Gestión de datos personales	Recolectar bases de datos
	Revisión de bases de datos
	Registro y actualización de las bases de datos
Oportunidades de mejoras SGSI	Reporte del estado de las Acciones Correctivas, correcciones y Oportunidades de Mejora

GESTIÓN	ACTIVIDADES
	Realizar seguimiento a las oportunidades de mejora producto de revisiones internas y externas a los Procesos
Planeación	Revisión Manual Políticas de Seguridad de la Información y documentos asociados

HISTORIAL DE CAMBIOS		
Fecha	***Versión***	***Descripción***
29/01/2020	1	Primera Versión del Documento.
29/01/2021	2	Segunda versión del documento. Se actualiza versión por cambios organizacionales y normativos, entre otros, la transición de la política de Gobierno En Línea por la Política de Gobierno Digital.
15/03/2022	3	Tercera versión del documento.
23/01/2023	4	Cuarta versión del documento. Se elabora este documento como parte de la implementación de la gestión de riesgos de seguridad digital para asegurar la confidencialidad, integridad y disponibilidad de los activos de información.
17/01/2024	5	Quinta versión del documento. Se realiza actualización y creación de nuevos apartes del presente documento como parte de la implementación de la gestión de riesgos de seguridad digital con el fin de articular las capacidades institucionales en el aseguramiento de la confidencialidad, integridad y disponibilidad de los activos de información.
2025	6	Sexta versión: Se realiza actualización y creación de nuevos apartes del presente documento como parte de la implementación de la identificación y gestión de riesgos de seguridad de la información con el fin de articular las capacidades institucionales en el aseguramiento de la confidencialidad, integridad y disponibilidad de los activos de información.

Elaboró: Andrea Linney Sierra Ladino **Cargo:** Contratista – Subdirección de Sistemas de Información de Tierras	**Revisó:** Diana Lucia Herrera Riaño	**Aprobó:** Comité Institucional de Gestión y Desempeño (Resolución 183 de 2018)
Firma: ORIGINAL FIRMADO **Elaboró:** Rosa Johanna Rincón Molina **Cargo:** Contratista – Subdirección de Sistemas de Información de Tierras	**Cargo:** Subdirectora de Sistemas de Información de Tierras	**Cargo:** Comité Institucional de Gestión y Desempeño, Sesión 1 del 23 de enero de 2025.
Firma: ORIGINAL FIRMADO	**Firma:** ORIGINAL FIRMADO	**Firma:** ACTA FIRMADA