PLAN DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2024

DIRECCIÓN DE GESTION DEL ORDENAMIENTO SOCIAL DE LA PROPIEDAD

SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN DE TIERRAS

CONTENIDO

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 riesgo que 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

Establecer un Plan de Gestión de Seguridad y Privacidad de la Información que apoye la creación e implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en la Agencia Nacional de Tierras, teniendo en cuenta los requerimientos del modelo de seguridad de la estrategia de Gobierno Digital, los requerimientos del negocio de la ANT, y el cumplimiento a las disposiciones legales vigentes nacionales e internacionales

3.2. Objetivos específicos

- Definir las etapas para establecer la estrategia de seguridad y privacidad de la información y el SGSI en la ANT.
- Optimizar la gestión de la seguridad de la información al interior de la ANT.
- Desarrollar la ejecución para la implementación del Sistema de Gestión de Seguridad de la Información de la ANT de acuerdo con los requerimientos establecidos en el modelo de seguridad 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, con una proyección hasta el 2024.

Las temáticas que serán cubiertas por el plan de gestión son:

- Diseño e Implementación del Sistema de Gestión de Seguridad de la Información - SGSI
- Definición y clasificación de activos de Seguridad de la Información
- Detección, análisis y tratamiento de Riesgos de Seguridad de la Información
- Control Acceso a la información
- Control de Seguridad perimetral
- Transferencia segura de la información
- Monitoreo de eventos de seguridad
- Seguridad en redes y comunicaciones
- Ciberseguridad
- Seguridad en proyectos de TI
- Gestión de vulnerabilidades
- Continuidad del negocio
- Capacitación y sensibilización en Seguridad de la Información.

5. BASE LEGAL

- Constitución Política de Colombia. Artículos 15, 20, 23 y 74.
- 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 1437 de 2011. Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.
- Ley 1474 de 2011. Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- • 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 88 de 2022. Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 Y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea.

- Decreto 620 de 2020. Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011, los literales e), j) y literal a) del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9° del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- Decreto 2106 de 2019. Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
- 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.
- 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:

• Dirección de Gestión del Ordenamiento Social de la Propiedad.

• Subdirección de Sistemas de Información de Tierras.

• Equipo de Infraestructura y Soporte Tecnológico – EIST de la Secretaria General.

• Mesa Técnica de TI.

• Áreas de procesos.

• Subdirección de Talento Humano.

• Profesional experto en seguridad informática.

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	70%	100%	GESTIONADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	36%	100%	REPETIBLE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	36%	100%	REPETIBLE
A.8	GESTIÓN DE ACTIVOS	31%	100%	REPETIBLE
A.9	CONTROL DE ACCESO	58%	100%	EFECTIVO
A.10	CRIPTOGRAFÍA	30%	100%	REPETIBLE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	30%	100%	REPETIBLE
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	49%	100%	EFECTIVO
A.15	RELACIONES CON LOS PROVEEDORES	30%	100%	REPETIBLE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	46%	100%	EFECTIVO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	34%	100%	REPETIBLE
A.18	CUMPLIMIENTO	49%	100%	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		43%	100%	EFECTIVO

Tabla 1. Resultados de evaluación de efectividad de controles.

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

Conforme al análisis y los resultados obtenidos, la puntuación promediada de los controles dentro de la entidad fue de 43%, lo cual muestra que la entidad se halla en un proceso “Efectivo” de medidas para la seguridad y privacidad de la información.

El análisis revela que existe una oportunidad de mejora en diversos aspectos de la gestión de la seguridad de la información los cuales son:

- Criptografía, Seguridad física del entorno y Relación con los proveedores, cuya puntación es del 30%
- Gestión de activos, que tiene una puntuación del 31%
- Seguridad de la información en la gestión de la continuidad del negocio, cuya puntación es del 34%
- Organización de la seguridad de la información y Seguridad de los recursos humanos, cuya puntación es del 36%.

La puntuación total alcanzada es 43% sobre la calificación objetivo de 100%

El grafico 1 contrasta el estado actual de los dominios de la norma ISO/EC 27001:2013 evaluados en la entidad, los cuales se representan con color verde y se contrasta con el estado ideal representado con color café.

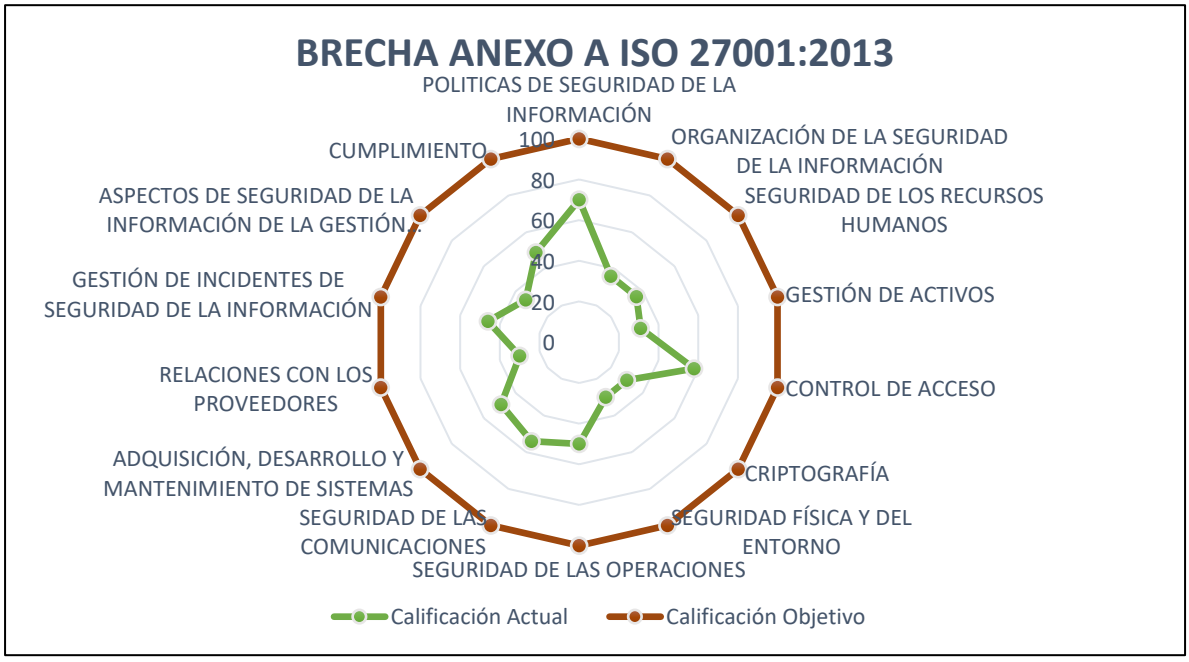

Gráfico 1. Brecha anexo ISO27001:2013. Fuente: Modelo de Seguridad y Privacidad de la Información – MSPI ANT Portada

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

No	Estrategia	Actividad	Responsable
1	Creación e Implementación Sistema de Gestión de Seguridad de la Información – SGSI	Se debe implementar el SGSI proyectando su ejecución hasta el 2025, llevar registros y evidencias de su implementación, así como demostrar la verificación e implementación de la mejora continua.	SSIT, EIST
2	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.	SSIT, EIST
3	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.	SSIT, EIST
4	Riesgos de Seguridad de la Información	Se deben llevar a cabo la identificación, valoración y planes de tratamiento de riesgos haciendo un seguimiento permanente, realizar revisiones periódicas de seguridad que permitan identificar nuevos riesgos, por lo tanto, estas acciones deben ser dinámicas durante la vigencia del plan de seguridad	SSIT, EIST
5	Acceso a la Información	Se debe construir los lineamientos de aseguramiento de credenciales para el acceso a los recursos compartidos y sistemas de información.	SSIT, EIST
6	Seguridad Perimetral	Se debe 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.	SSIT, EIST
7	Transferencia Segura de la Información	Se deben 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.	SSIT, EIST
8	Monitoreo de eventos de Seguridad	Teniendo en cuenta los indicadores de gestión, se recomienda generar una herramienta que permita documentar el proceso monitoreo de seguridad.	SSIT, EIST
9	Seguridad en redes y comunicaciones	Garantizar el servicio web sobre HTTPS, así mismo, se deben realizar unas 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	SSIT, EIST

10	Seguridad en proyectos de TI	se debe considerar desde los mismos RFIs o RFPs los requisitos de seguridad que se debe atender para cada caso, y luego tener en cuenta las cláusulas que apliquen, como temas de confidencialidad, auditoria de los servicios brindados, etc. En caso de que se adquieran equipos o soluciones, se debe exigir temas como: OWASP o estándar de verificación de Seguridad en las aplicaciones, roles y perfiles, Logs de Auditoria, Guías de Aseguramiento, Pruebas de Vulnerabilidades, entre otros	SSIT, EIST
11	Gestión de Vulnerabilidades	Se deben generar estándares de seguridad de la plataforma tecnológica, para realizar el correspondiente hardening, luego hacer pruebas de vulnerabilidades y llevar a cabo los planes de tratamiento de las vulnerabilidades identificadas, dándole prioridad a las críticas altas continuar con las medias y bajas	SSIT, EIST
12	Continuidad del Negocio	Se debe llevar a cabo 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.	SSIT, EIST
13	Capacitación y Sensibilización en Seguridad de la Información	mantener de manera periódica las campañas de sensibilización en temas de seguridad de la información, así mismo, cada año se debe proponer cursos de actualización en temas de seguridad, con el fin de que se mantengan al día en cuanto a las nuevas brechas de seguridad	SSIT, EIST
14	Privacidad y protección de información de datos personales	Realizar de manera periódica las campañas de privacidad de protección de datos personales, así mismo, se debe realizar auditorías que permitan establecer el cumplimiento de la ley.	SSIT, EIST

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.

Elaboró:	**Revisó:**	**Aprobó:** Comité Institucional de Gestión y Desempeño (Resolución 183 de 2018)
Andrea Linney Sierra Ladino	Diana Lucia Herrera Riaño	
Cargo: Contratista – Secretaría General	**Cargo:** Subdirectora Sistemas de Información de Tierras	**Cargo:** Comité Institucional de Gestión y Desempeño, Sesión 1 del 17 de enero de 2024
Firma:	**Firma:**	**Firma:**
ORIGINAL FIRMADO	ORIGINAL FIRMADO	ACTA FIRMADA