POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

DIRECCIÓN DE GESTIÓN DEL ORDENAMIENTO SOCIAL DE LA PROPIEDAD

SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN DE TIERRAS

TABLA DE CONTENIDO

1. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 3
2. PREMISAS POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 3
3. OBJETIVOS DE LA POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 4
4. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN. 5
5. ÁMBITO DE APLICACIÓN 5
6. ALCANCE. 5
7. REVISIONES Y/O ACTUALIZACIONES. 5
8. COMPROMISO DE LA DIRECCIÓN 6

1. 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 y preservación de la confidencialidad, integridad y disponibilidad de los diferentes activos de información (de tipo información, hardware, software, redes, servicios, procesos y personas), para lo cual mediante la adopción del Modelo de Seguridad de la Información implementado a través del Sistema de Gestión de Seguridad de la Información institucional que se encuentra alineado con el estándar ISO 27001, realiza la gestión de riesgos de seguridad de la información y propende por la generación de cultura e implementación de buenas prácticas de seguridad de la información.

2. PREMISAS POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para el cumplimiento de la Política General de Seguridad y Privacidad de la Información se definen las siguientes premisas:

- Definir, implementar, operar y mejorar de forma continua el Sistema de Gestión de Seguridad de la Información - SGSI, como herramienta para identificar y mitigar los riesgos sobre la información institucional, garantizando la aplicación de los controles requeridos para proteger los activos de información según la declaratoria de aplicabilidad de la Entidad.

- Definir, mantener y actualizar los requisitos de seguridad asociados al contexto de la ANT, para lo cual se debe revisar y mantener la documentación del Sistema de Gestión de Seguridad de la Información (SGSI) de la ANT actualizada, vigente y operativa, de acuerdo con las necesidades de la Entidad y procurando que todas las partes involucradas la conozcan y apliquen.

- Definir y capacitar sobre las responsabilidades asociadas a seguridad de la información al funcionarios, contratistas y terceros que tiene relación con el manejo de los activos de información de la ANT, asegurando la existencia de competencias requeridas para la ejecución de las tareas asignadas.

- Comunicar efectivamente los aspectos asociados al Sistema de Gestión de Seguridad de la Información a todas las partes involucradas, generando una cultura de seguridad de la información.

- Garantizar la seguridad de la información en las actividades de definición de programas, proyectos, planes, objetivos, y otros generados a partir de los procesos de direccionamiento estratégico de la ANT.

- Definir y mantener lineamientos, estándares, procedimientos u otras herramientas que permitan abordar la seguridad de la información a partir de los dominios de seguridad definidos en el Modelo de Seguridad y Privacidad de la Información y la Norma ISO 27001, a efectos de asegurar su vigencia, nivel de eficacia y conformidad con las orientaciones estratégicas de la Entidad. Asegurar la protección y privacidad de la información y darle un manejo apropiado, al igual que a los diferentes tipos de activos que interactúan con la información custodiada por la ANT.

- Asegurar la protección y privacidad de la información administrada por la entidad y darle un manejo apropiado, al igual que a los diferentes tipos de activos que interactúan con la información custodiada por la ANT.

- Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos, mediante la implementación de controles de acceso a la información, sistemas y recursos de red.

- Controlar la operación de los procesos de negocio, garantizando la seguridad de los recursos tecnológicos y las redes de datos.

- Cumplir con los requerimientos legales para la seguridad y privacidad de la información, definidos por la normatividad aplicable a la Entidad.

- Fortalecer la capacidad institucional para Identificar, Proteger, Detectar, Responder y Recuperar ante un ciberataque.

3. OBJETIVOS DE LA POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

3.1 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).**

3.2 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).**

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

3.4 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).**

3.5 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).**

4. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN.

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

5. ÁMBITO DE APLICACIÓN

El cumplimiento de la Política General de Seguridad y Privacidad de la Información y las Políticas Específicas de Seguridad de la Información, es obligatorio para los funcionarios, contratistas, proveedores y, en general, cualquier usuario que tenga relación con los activos de información institucionales. En caso de violaciones a estas, la Entidad se reserva el derecho de tomar las medidas administrativas, contractuales y/o disciplinarias a que exista lugar.

6. ALCANCE.

Esta política aplica a todos los procesos estratégicos, misionales, de apoyo y de evaluación de la Entidad, así como a todos los funcionarios, contratistas, terceros, servicios, sistemas de información y a los activos de información que apoyan la operación de la Agencia Nacional de Tierras

7. REVISIONES Y/O ACTUALIZACIONES.

Las políticas de seguridad de la información serán sometidas a revisión y actualización con una periodicidad anual o cuando se presenten cambios significativos en el contexto interno y/o externo de la Entidad.

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

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

8. COMPROMISO DE LA DIRECCIÓN

La Alta Dirección de la Agencia Nacional de Tierras – ANT, en cumplimiento de la Política de Seguridad de la Información y Gobierno Digital, se compromete a implementar el Sistema de Gestión de Seguridad de la Información – SGSI, asegurando el respaldo necesario en recursos humanos, técnicos y financieros para cumplir con las normativas del Ministerio de Tecnologías de la Información y las Comunicaciones, y los decretos que lo soportan. Además, de promover la mejora continua del SGSI y fomentar el compromiso institucional entre los funcionarios, contratistas y terceros.

HISTORIAL DE CAMBIOS		
Fecha	**Versión**	**Descripción**
14/09/2017	1	Primera versión del documento.
24/09/2018	2	Segunda versión del documento.
01/02/2019	3	Tercera Versión. Actualización del lineamiento para contemplar actualización de la política de gobierno digital de MINTIC
19/09/2022	4	Cuarta Versión. Se actualiza versión por cambios organizacionales y del entorno.
07/10/2024	5	Quinta Versión, Se actualiza versión por restructuración del documento.

Elaboró: Jorge Luis Vargas Buitrago	**Revisó:** Diana Lucia Herrera Riaño	**Aprobó:** Sesión 3 Comité Institucional de Gestión y Desempeño 07/10/2024
Cargo: Contratista	**Cargo:** Subdirectora de Sistemas de Información de Tierras	
Firma: ORIGINAL FIRMADO	**Firma:** ORIGINAL FIRMADO	

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

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