POLÍTICA GESTIÓN DE VULNERABILIDADES Y ASEGURAMIENTO DE PLATAFORMA

DIRECCIÓN DE GESTIÓN DEL ORDENAMIENTO SOCIAL DE LA PROPIEDAD

SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN DE TIERRAS

DICIEMBRE 2025

GESTIÓN DE VULNERABILIDADES Y ASEGURAMIENTO DE PLATAFORMA

1. INTRODUCCIÓN

En el entorno digital actual, las entidades públicas enfrentan desafíos crecientes asociados a la protección de la información, la disponibilidad de los servicios y la resiliencia frente a amenazas cibernéticas. La identificación temprana, el análisis y la atención oportuna de vulnerabilidades en la infraestructura tecnológica se han convertido en una condición indispensable para salvaguardar la continuidad operativa, cumplir las obligaciones normativas y garantizar la confianza de la ciudadanía en los servicios prestados por el Estado.

En esta línea, la Agencia Nacional de Tierras (ANT), a través de la Subdirección de Sistemas de Información de Tierras, reconoce la importancia estratégica de adoptar prácticas formales, sistemáticas y sostenibles para la gestión de vulnerabilidades en los activos de información, plataformas, servicios, redes, bases de datos, aplicaciones y demás componentes críticos que soportan la operación institucional. Por ello, se establece la presente Política de Gestión de Vulnerabilidades, como un marco orientador para la identificación, evaluación, priorización, tratamiento, remediación y seguimiento continuo de las debilidades técnicas que puedan afectar la seguridad o disponibilidad de los servicios tecnológicos de la entidad.

Las vulnerabilidades pueden surgir por múltiples factores: errores de configuración, software desactualizado, fallas en componentes de hardware, debilidades en el desarrollo de aplicaciones, exposición indebida en servicios de red, uso de tecnologías obsoletas o nuevas amenazas conocidas públicamente (incluyendo zero-day). En todos los casos, su adecuada gestión debe considerar el análisis del riesgo asociado, la criticidad de los activos afectados, el nivel de exposición, la disponibilidad de alternativas de mitigación y el cumplimiento de estándares y lineamientos nacionales e internacionales en materia de seguridad de la información.

Esta política promueve una visión preventiva, integral y colaborativa, involucrando a las áreas responsables de infraestructura, seguridad de la información, arquitectura, desarrollo, servicios tecnológicos y terceros que administren activos institucionales. Así mismo, establece mecanismos claros de coordinación, reporte, documentación y control, que permitan reducir la superficie de ataque, minimizar la probabilidad de explotación de vulnerabilidades y fortalecer la postura de seguridad institucional. Con ello, la ANT reafirma su compromiso con la mejora continua y la protección de sus activos de información, garantizando servicios confiables y alineados con los principios de seguridad, eficiencia y modernización del Estado.

2. OBJETIVO GENERAL

Establecer los lineamientos para la gestión integral de vulnerabilidades en los activos de información, infraestructura tecnológica, aplicaciones, plataformas y servicios de la Agencia Nacional de Tierras (ANT), con el fin de identificar, evaluar, priorizar, tratar y monitorear las debilidades técnicas que puedan afectar la seguridad, continuidad operativa y resiliencia institucional, asegurando una respuesta oportuna, coordinada y trazable frente a los riesgos asociados.

2.1. Objetivos específicos:

- Definir el marco de actuación para la gestión de vulnerabilidades que afecten sistemas de información, infraestructura tecnológica, componentes en la nube, bases de datos, redes, aplicaciones y demás activos críticos de la ANT.

- Establecer un proceso formal y repetible para la identificación, análisis, clasificación, priorización, tratamiento, remediación y verificación de las vulnerabilidades detectadas.

- Promover la participación coordinada de las áreas responsables de infraestructura, seguridad de la información, desarrollo, arquitectura, proveedores externos y otros actores involucrados, para asegurar decisiones informadas y coherentes frente al tratamiento de cada vulnerabilidad.

- Garantizar que las vulnerabilidades sean gestionadas de manera oportuna, evitando afectaciones a la disponibilidad, confidencialidad, integridad, trazabilidad, autenticidad y desempeño de los servicios tecnológicos de la entidad.

- Impulsar la documentación y trazabilidad de todo el ciclo de gestión de vulnerabilidades, incluyendo hallazgos, riesgos asociados, decisiones, acciones de remediación y validaciones, con el fin de fortalecer la auditoría, la mejora continua y el cumplimiento normativo.

- Asegurar la alineación con estándares, buenas prácticas y marcos normativos, incluyendo lineamientos del MSPI, instrumentos de seguridad del Estado, estándares internacionales (ISO/IEC 27001, NIST) y recomendaciones de los fabricantes y comunidades de seguridad.

- Promover un enfoque preventivo de ciberseguridad, reduciendo la superficie de ataque, incrementando la resiliencia institucional y contribuyendo a la protección de los activos de información bajo la responsabilidad de la ANT.

3. ALCANCE

La presente política aplica a todas las pruebas, análisis, remediaciones y actividades que impacten los componentes tecnológicos y de información de la Agencia Nacional de Tierras (ANT), incluyendo, pero sin limitarse a:

- Infraestructura tecnológica (servidores, redes, comunicaciones, centros de datos, dispositivos de almacenamiento y seguridad perimetral).
- Sistemas de información y sus módulos funcionales.
- Bases de datos y servicios asociados.
- Plataformas en la nube, entornos virtualizados y servicios tecnológicos tercerizados.
- Herramientas de monitoreo, gestión de identidad, seguridad de la información y continuidad del negocio.
- Equipos de usuario final cuando el cambio afecte servicios compartidos o críticos para la operación institucional.

Este lineamiento es de aplicación obligatoria para todos los equipos técnicos responsables de la implementación, mantenimiento, soporte o evolución de los servicios tecnológicos, incluyendo funcionarios, contratistas y proveedores externos que presten servicios bajo contratos vigentes con la entidad.

4. NORMATIVIDAD Y MARCOS DE REFERENCIA

Esta política se fundamenta en el marco legal colombiano y en buenas prácticas internacionales para la gestión de la seguridad de la información, la seguridad digital y, en particular, la gestión de vulnerabilidades en los servicios de tecnología e información. A continuación, se detallan los lineamientos, normas y marcos de referencia considerados para su elaboración:

4.1. Marco legal colombiano

- Ley 1437 de 2011 (Código de Procedimiento Administrativo y de lo Contencioso Administrativo): En lo relacionado con el uso, gestión y trazabilidad de los sistemas de información públicos.

- Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal y se crea el bien jurídico “protección de la información y de los datos”, tipificando los delitos informáticos y protegiendo integralmente los sistemas que utilizan TIC.

- Ley 1581 de 2012 y sus decretos reglamentarios: Por la cual se dictan disposiciones generales para la protección de datos personales.

- Ley 1712 de 2014: Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, relevante para la gestión de la información pública y su protección.

- Decreto 1078 de 2015: Decreto Único Reglamentario del Sector TIC, que compila la regulación aplicable al sector y articula temas de gobierno digital y seguridad de la información.

- Decreto 1499 de 2017: Por el cual se modifica el Decreto 1083 de 2015 en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015, adoptando y formalizando el Modelo Integrado de Planeación y Gestión – MIPG.

- Modelo Integrado de Planeación y Gestión – MIPG: Como marco para la gestión y desempeño institucional en entidades públicas, dentro del cual se inserta la gestión de seguridad de la información y seguridad digital.

4.2. Políticas y lineamientos nacionales de seguridad digital y gobierno digital

- Política de Gobierno Digital del MinTIC: Instrumento de política pública que orienta la transformación digital del Estado y la prestación de servicios apoyados en TIC, incluyendo el habilitador de seguridad y privacidad de la información.

- Política de Seguridad Digital / Política Nacional de Seguridad Digital (CONPES 3854 de 2016): Establece la política nacional de seguridad digital, definiendo objetivos y líneas de acción para fortalecer las capacidades del país en materia de seguridad digital.

- Política Nacional de Confianza y Seguridad Digital (CONPES 3995 de 2020): Actualiza y profundiza la política nacional de seguridad digital, orientada a desarrollar la confianza digital mediante el fortalecimiento de la seguridad digital y sus capacidades institucionales.

- CONPES 3701 de 2011 – Lineamientos de Política para Ciberseguridad y Ciberdefensa: Define lineamientos de política para fortalecer las capacidades del Estado frente a amenazas en el ciberespacio.

- CONPES 3975 de 2019 – Política Nacional para la Transformación Digital y la Inteligencia Artificial: En lo relacionado con la transformación digital del Estado y el uso estratégico de tecnologías digitales, que impactan directamente la gestión de riesgos y vulnerabilidades.

- Resolución 500 de 2021 del MinTIC (corrección de año): “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el Modelo de Seguridad y Privacidad de la Información (MSPI) como habilitador de la Política de Gobierno Digital”.

- Resolución 746 de 2022 del MinTIC: 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 500 de 2021, especialmente en materia de relaciones con proveedores y servicios en la nube.

- Modelo de Seguridad y Privacidad de la Información – MSPI (documentos y guías vigentes): Como marco de referencia para la gestión de la seguridad y privacidad de la información y la seguridad digital, alineado con estándares internacionales y estructurado en fases para la gestión del ciclo de vida de la seguridad de la información.

4.3. Estándares y buenas prácticas internacionales

- ISO/IEC 27001:2022 – Sistemas de Gestión de Seguridad de la Información (SGSI): Como estándar de referencia para el establecimiento, implementación, mantenimiento y mejora continua de un SGSI alineado con la gestión de vulnerabilidades.

- ISO/IEC 27002:2022 – Controles de Seguridad de la Información, ciberseguridad y protección de la privacidad: Referente para la selección e implementación de controles de seguridad de la información, incluyendo controles de gestión de vulnerabilidades, parches y seguridad técnica.

Guías y publicaciones del NIST (National Institute of Standards and Technology), en particular:

- NIST SP 800-40 – Guide to Enterprise Patch Management Planning / Creating a Patch and Vulnerability Management Program, como referencia específica para la gestión de parches y vulnerabilidades.

Marcos y catálogos técnicos de vulnerabilidades, tales como:

- CVE (Common Vulnerabilities and Exposures) y

- CVSS (Common Vulnerability Scoring System), utilizados como referencia para la identificación, clasificación y priorización de vulnerabilidades a nivel internacional.

5. DOCUMENTOS INTERNOS DE REFERENCIA

5.1. Políticas estratégicas transversales aplicables

- **INTI-Política-001**: Política de Seguridad de la Información
- **INTI-Política-002**: Política General de Infraestructura TIC
- **INTI-Política-003**: Política General de Sistemas de Información
- **INTI-Política-004**: Política General de la Gestión de Datos e Información
- **INTI-Política-005**: Política General de Servicios TIC
- **INTI-Política-006**: Política General de la Estrategia TIC
- **INTI-Política-008**: Política de lineamientos de Seguridad de la Información (versión 4)

5.2. Procedimientos estratégicos de apoyo

- **INTI-P-003: Arquitectura TIC**
- **INTI-P-004: Gobierno de TIC**
- **INTI-P-005: Planeación Estratégica de TIC**
- **INTI-P-006: Gestión de la Continuidad del Negocio**

5.3. Documentos misionales directamente relacionados con control de cambios

- **GINFO-Política-002**: Lineamientos para el Desarrollo de Productos de Software
- **GINFO-P-003**: Procedimiento de Construcción de Software
- **GINFO-P-011**: Procedimiento de Gestión de Incidentes de Seguridad de la Información
- **GINFO-P-014**: Gestión de Parches y Actualizaciones
- **GINFO-P-019**: Gestión transversal de cambios en los componentes de tecnología e información
- **GINFO-PT-002**: Protocolo de Paso a Producción

5.4. Documentos de soporte complementarios

- **GINFO-F-033**: Lista de Chequeo Paso a Producción
- **GINFO-F-031**: Formato de Solicitud de Requerimientos de Software
- **GINFO-F-029**: Formato de Mantenimiento Preventivo, Correctivo y Evolutivo de Componentes de Infraestructura
- **GINFO-F-032**: Formato de Análisis de Requerimientos
- **GINFO-I-015**: Instructivo de Buenas Prácticas en ITIL para la Gestión de los Servicios de TI
- **GINFO-M-007**: Manual para la gestión de cambios o actualizaciones de TI

6. DEFINICIONES

- **Activo de información**: Cualquier dato, sistema, servicio, infraestructura, hardware o software que tiene valor para la entidad y requiere protección.
- **Análisis de vulnerabilidades**: Proceso sistemático para identificar, evaluar y priorizar vulnerabilidades en sistemas, aplicaciones, dispositivos y redes.
- **Áreas críticas**: Dependencias institucionales cuyas funciones o información manejada requieren niveles reforzados de seguridad, por lo que los equipos asignados deben cumplir estándares más estrictos de aseguramiento.
- **Aseguramiento de plataforma (Hardening)**: Proceso de aplicar configuraciones, controles y prácticas de seguridad destinadas a reducir la superficie de ataque de un sistema, eliminando servicios innecesarios, configuraciones por defecto, usuarios predefinidos, puertos abiertos sin uso y cualquier elemento que aumente el riesgo de explotación.
- **Auditoría de configuración**: Proceso mediante el cual el equipo de Seguridad de la Información verifica la correcta aplicación de las plantillas de aseguramiento y la adherencia a los estándares definidos para cada plataforma.
- **Backdoor (Puerta trasera)**: Mecanismo oculto o no autorizado que permite acceso remoto o control de un sistema sin pasar por los procedimientos normales de autenticación.
- **CAS (Centro de Atención y Soporte / Mesa de Ayuda)**: Plataforma institucional de reporte, registro y seguimiento de solicitudes, incidentes, requerimientos funcionales y técnicos relacionados con los servicios de TI. En el contexto de esta política, es el canal oficial para que funcionarios y contratistas reporten hallazgos de vulnerabilidades o comportamientos anómalos en equipos, sistemas o procesos tecnológicos.
- **Ciberexposición**: Nivel de riesgo al que está expuesto un activo, sistema o entorno frente a amenazas cibernéticas, considerando criticidad, accesibilidad, entorno y valor del activo.
- **CIS Benchmarks (CISecurity)**: Guías de configuración segura desarrolladas por el Center for Internet Security (CIS) que establecen prácticas de endurecimiento ampliamente adoptadas para sistemas operativos, bases de datos, servicios de red, contenedores, nubes públicas y otros componentes tecnológicos.
- **CISO (Chief Information Security Officer)**: Oficial en Jefe de Seguridad de la Información encargado de establecer, coordinar y supervisar la estrategia y políticas de seguridad de la información.
- **Clasificación CVSS**: Sistema estándar para puntuar la severidad de vulnerabilidades basado en factores base, temporales y ambientales.
- **Colocation:** Modelo en el cual la entidad aloja sus propios servidores y equipamiento tecnológico en un centro de datos operado por un tercero. El proveedor suministra espacio físico, energía, climatización y seguridad física, mientras la entidad mantiene el control de sus equipos y de la gestión lógica de la infraestructura.
- **Configuración segura**: Conjunto de parámetros técnicos definidos por el equipo de Seguridad de la Información que garantizan que un sistema, servidor, base de datos, estación de trabajo o componente de red opera bajo estándares mínimos de seguridad.

- **CVE (Common Vulnerabilities and Exposures)**: Catálogo público estandarizado que identifica vulnerabilidades conocidas mediante un código único.
- **Ethical Hacking (Pruebas de intrusión/HE)**: Conjunto de pruebas autorizadas y controladas para identificar debilidades de seguridad mediante técnicas utilizadas por atacantes, sin causar daño a los sistemas.
- **Evidencia técnica**: Documentación verificable que demuestra una incompatibilidad o afectación generada por una configuración de aseguramiento, sustentada mediante pruebas, registros, análisis del sistema operativo o comportamiento de la plataforma.
- **Explotación**: Uso de una vulnerabilidad identificada para comprometer la confidencialidad, integridad, disponibilidad o control de un sistema.
- **Gestión de vulnerabilidades**: Ciclo completo que incluye identificación, análisis, priorización, tratamiento, remediación y seguimiento de vulnerabilidades.
- **Grupos de Hardening en Directorio Activo**: Conjuntos de políticas o grupos de seguridad definidos en Active Directory que aplican configuraciones de endurecimiento y restricciones específicas a usuarios o equipos de acuerdo con su sensibilidad o criticidad
- **Hallazgo**: Resultado documentado de un análisis de vulnerabilidades o prueba de intrusión que evidencia una debilidad técnica o control inefectivo.
- **Hardening**: Término en inglés utilizado para referirse al endurecimiento de sistemas o plataformas mediante la aplicación de configuraciones seguras, deshabilitación de funcionalidades no requeridas y fortalecimiento de controles de seguridad.
- **Instalaciones por defecto**: Configuraciones o servicios habilitados automáticamente por un sistema o software al momento de su instalación inicial, los cuales suelen incluir elementos inseguros o innecesarios que deben ser deshabilitados o ajustados.
- **Inventario de activos**: Registro actualizado y estructurado de los activos tecnológicos de la entidad, incluyendo sus atributos, propietarios, criticidad y estado.
- **Mitigación**: Acción destinada a reducir el riesgo asociado a una vulnerabilidad sin necesariamente eliminarla totalmente.
- **Nube privada**: Modelo de servicio en el cual la infraestructura tecnológica es utilizada de manera exclusiva por la entidad, ya sea operada internamente o por un tercero, y ofrece mayores niveles de control, seguridad y personalización frente al manejo de datos y servicios críticos.
- **Nube pública**: Modelo de computación en la nube ofrecido por proveedores externos (como AWS, Azure, GCP), donde los recursos tecnológicos —como almacenamiento, procesamiento y redes— se comparten entre múltiples clientes, manteniendo aislamiento lógico. Proporciona escalabilidad bajo demanda, disponibilidad global y costos optimizados.
- **Parche (Patch)**: Actualización de software que corrige vulnerabilidades, errores o fallas de seguridad.
- **Plantillas de aseguramiento (o Baselines de seguridad)**: Documentos o configuraciones estandarizadas que contienen los parámetros mínimos de seguridad que deben aplicarse a un tipo de plataforma tecnológica específica (servidores, bases de datos, estaciones de trabajo, etc.).
- **Política BYOD**: Lineamientos que regulan el uso de dispositivos personales por parte de contratistas y funcionarios para acceder a recursos institucionales.
- **Remediación**: Corrección definitiva de una vulnerabilidad identificada mediante actualizaciones, mejoras de configuración, reemplazo de componentes u otras acciones técnicas.
- **Revisión de configuraciones**: Proceso periódico mediante el cual se evalúa si las configuraciones seguras y las plantillas de aseguramiento continúan vigentes, efectivas y alineadas con las necesidades de la plataforma o con cambios tecnológicos.
- **Riesgo residual**: Nivel de riesgo que permanece después de aplicar controles o remediaciones.
- **Severidad**: Medida del impacto potencial de una vulnerabilidad si fuera explotada, generalmente clasificada como crítica, alta, media o baja.

- **SSIT (Subdirección de Sistemas de Información de Tierras)**: Dependencia de la Agencia Nacional de Tierras responsable de la gestión, administración, desarrollo, operación y soporte de los sistemas de información, plataformas tecnológicas, infraestructura y servicios digitales que soportan la operación misional y administrativa de la entidad. Actúa como instancia técnica y estratégica para la toma de decisiones en materia de transformación digital, seguridad de la información, arquitectura tecnológica y continuidad de los servicios.
- **Superficie de ataque**: Conjunto de puntos, servicios o interfaces que pueden ser aprovechados por un atacante para comprometer un sistema.
- **Usuarios por defecto**: Cuentas precreadas por los sistemas operativos, servicios, aplicaciones o bases de datos durante su instalación, que pueden representar un riesgo si no se deshabilitan, eliminan o fortalecen adecuadamente.
- **Zero-day**: Vulnerabilidad desconocida públicamente o sin parche disponible al momento de su descubrimiento.

7. DESCRIPCIÓN

7.1 LINEAMIENTOS GENERALES PARA LA GESTIÓN DE VULNERABILIDADES

Es responsabilidad de la Subdirección de Sistemas de Información de Tierras realizar la actualización, revisión y aprobación de los lineamientos descritos en el presente documento. Así mismo, es responsable de establecer el debido contacto con las autoridades y certificar a clientes/titulares/entidades sobre la gestión de acuerdo a los requerimientos contractuales o de cumplimiento que estén vigentes.

El Equipo de Infraestructura y Soporte Tecnológico - EIST de la Secretaría General deberá definir y actualizar trimestralmente el inventario de activos tecnológicos considerados críticos (internos y externos), de QA, Desarrollo y pruebas en los ambientes On-prem y Nube (privada, pública, colocation), que soporten la operación de la Agencia Nacional de Tierras, el cual deberá ser entregado al equipo de Seguridad de la Información para ejecutar las pruebas de análisis de vulnerabilidades según cronograma de ejecución definido a principio de cada año.

Es responsabilidad del equipo de Seguridad de la Información documentar los hallazgos identificados después de cada prueba de análisis de vulnerabilidades, teniendo como premisa que las vulnerabilidades identificadas deberán estar homologadas por el CVE (*Common Vulnerabilities and Exposures*), deben tener una metodología de puntaje y permitir el análisis de ciberexposición.

El alcance de las pruebas de análisis de vulnerabilidades solo contempla dispositivos tecnológicos pertenecientes a la Agencia Nacional de Tierras, los dispositivos tecnológicos de proveedores, clientes o cualquier entidad que no pertenezca a la Agencia Nacional de Tierras **NUNCA** deben ser incluidos en los análisis de vulnerabilidades, a menos que la tercera parte este de acuerdo y se haya definido a nivel contractual o se solicite formalmente al Oficial de Seguridad de la Información y Seguridad Digital (definido como Chief Information Security Officer en adelante CISO, que traducido al español significa Oficial en Jefe de Seguridad de la Información y que aparece de forma homónima en diferentes normas de referencia en inglés y español), definiendo el alcance, activos, ventanas de tiempo y necesidades.

El análisis de vulnerabilidades a dispositivos personales de contratistas se realizará mediante escáneres o agentes, siempre que estén en las instalaciones de la Agencia Nacional de Tierras o conectados a su red mediante conexiones inalámbricas o por VPN, por lo cual es indispensable mantener aislados los datos privados de los de la agencia en dichos equipos, tal como se define en la política BYOD (Bring Your Own Device, traducido al español como Trae tu propio dispositivo) de la Entidad. La Agencia Nacional de Tierras se reserva el derecho de aislar y/o contener equipo

y usuarios que muestren comportamientos o vulnerabilidades que puedan afectar la infraestructura, información o datos de y a cargo de la entidad y se reportarán por parte del equipo de Seguridad de la Información, el SOC, NOC u otras áreas que la detecten y se procederá a la ejecución de los procedimientos de gestión de eventos e incidentes de seguridad de la información incluyendo el reporte a entes gubernamentales como COLCERT.

El análisis de vulnerabilidades a dispositivos personales de contratistas y funcionarios de manera remota estará disponible para su ejecución, previa autorización firmada por el contratista y/o funcionario como parte de las políticas BYOD de la Entidad

Es responsabilidad de los Directores, Sub-Directores, Líderes de áreas y dependencias, ejecutar las acciones pertinentes para mitigar los riesgos ocasionados por las amenazas detectadas en las pruebas de análisis de vulnerabilidades, según la criticidad de las mismas.

Bajo ninguna circunstancia se permitirá que un tercero, persona natural o jurídica incluyendo clientes, proveedores estratégicos, aliados, etc., realicen escaneos de vulnerabilidades o pruebas de penetración (hacking ético) de cualquier índole, sin la autorización expresa del/la Líder de Seguridad Informática, el jefe de seguridad de la información o CISO.

7.2 Periodicidad

Para los dispositivos ubicados en la red externa (servidores y equipos de comunicación), la periodicidad de ejecución de pruebas de vulnerabilidades será trimestral, definiendo cada ejecución como Q (del inglés Quarter), teniendo cuatro Q al año.

Para las aplicaciones web internas o externas, la periodicidad de ejecución de pruebas de vulnerabilidades será trimestral, definiendo cada ejecución como Q (del inglés Quarter).

Para los dispositivos ubicados en la red interna (servidores, equipos de comunicación y estaciones de trabajo), la periodicidad de ejecución de pruebas de vulnerabilidades será trimestral, definiendo cada ejecución como Q (del inglés Quarter).

Toda solicitud de análisis de vulnerabilidades a nuevos desarrollos, proyectos, actualizaciones y/o despliegues tecnológicos, realizada por correo electrónico al Equipo de Seguridad de la Información, se tendrá en cuenta para el informe trimestral de análisis de vulnerabilidades en el cual se realizó la solicitud.

Las pruebas de intrusión (Ethical Hacking) deben ejecutarse como mínimo con una periodicidad semestral y deben incluir pruebas a las redes inalámbricas, pruebas de ingeniería social (p.e., escritorio limpio, Dumpster Diving - búsqueda de información sensible en elementos de disposición final-, etc.) y Pruebas a las aplicaciones WEB de la entidad.

Se debe ejecutar análisis de vulnerabilidades al direccionamiento externo después de cualquier cambio sobre los componentes expuestos en la red pública.

7.3 Proceso análisis de vulnerabilidades

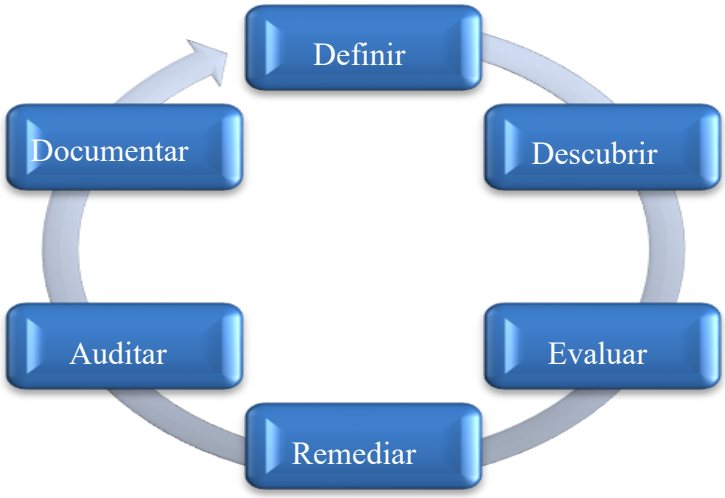

Ilustración 1. Proceso de análisis de vulnerabilidades

1. **Definir:** Políticas, procedimientos y alcance.
2. **Descubrir:** Identificar y priorizar los activos.
3. **Evaluar:** Ejecución de escaneo en sistemas y dispositivos.
4. **Remediar:** Diseñar y ejecutar planes de acción para remediar las vulnerabilidades identificadas.
5. **Auditar:** Ejecutar nuevamente escaneos luego de ejecutar remediaciones, o después de cualquier cambio representativo en la red.
6. **Documentar:** Diligenciar y mantener las evidencias de las remediaciones.

7.4 Proceso Ethical Hacking, con autorización previa formal

Ilustración 2 Procedimiento de pruebas de Ethical Hacking

1. **Escaneo de redes:** Identificación de equipos activos en los rangos internos/externos de red dados; en esta actividad se debe revisar que las segmentaciones de red estén configuradas correctamente.
2. **Escaneos de puertos y servicios:** Identificación de entradas habilitadas para acceso sobre el dispositivo evaluado y los servicios prestados.
3. **Enumeración de información:** Identificación de banners (letreros o descripciones de servicios que informan la naturaleza y posible configuración de un servidor), cuentas de correo, usuarios, etc.
4. **Identificación de vulnerabilidades:** Validar las vulnerabilidades vigentes para cada servicio y plataforma teniendo en cuenta versiones de sistema operativo y actualizaciones, entre otros.
5. **Explotación de vulnerabilidades sobre puertos y servicios habilitados:** Ejecución de ataques controlados y orientados a vulnerar aquellas entradas identificadas. Esta actividad se realiza sobre aquellas vulnerabilidades que no afectan el servicio y que pueden ser explotadas sin causar fallas en el sistema, de lo contrario se evaluará el impacto directamente con el cliente para programar la realización de las mismas en horarios o ventanas de tiempo específicos.
6. **Elevación de privilegios:** Búsqueda del control total del dispositivo evaluado (apoderamiento de la máquina), en los casos en donde sea posible.

7.5 Remediación análisis de vulnerabilidades

Los niveles de impacto de las vulnerabilidades identificadas en los escaneos de análisis de vulnerabilidades deberán reportarse bajo las siguientes definiciones, y se deberán realizar planes de acción de remediaciones para las vulnerabilidades de tipo Crítica, Alta y Media en los tiempos establecidos en la presente política. Esta denominación debe coincidir con la clasificación de la herramienta de Escaneo de vulnerabilidades corporativa.

Severidad	Descripción	Remediación
Crítica	Un delincuente/intruso informático puede obtener fácilmente el control total del dispositivo afectado, lo cual puede afectar directamente el compromiso de toda la red corporativa. Por ejemplo, las vulnerabilidades de este nivel de severidad contemplan el acceso completo de lectura y acceso de escritura a los archivos, ejecución remota de comandos, y la presencia de puertas traseras (*Backdoors*), APTs (Amenazas Avanzadas Persistentes – *Advanced Persistent Threats*).	15 Días
Severidad	Descripción	Remediación
Alta	Existe gran posibilidad que un delincuente/intruso informático tome control total del dispositivo afectado, lo cual puede generar fugas de información sensible. Por ejemplo, las vulnerabilidades en este nivel pueden incluir el acceso completo de lectura a los archivos, puertas traseras potenciales, o una lista de todos los usuarios.	30 Días

Media	Un delincuente/intruso informático puede obtener acceso a información específica almacenada en el dispositivo afectado, incluyendo la configuración de seguridad. Las vulnerabilidades en este nivel pueden incluir la divulgación parcial del contenido de archivos, exploración de directorios, la divulgación de las reglas de filtrado y mecanismos de seguridad, ataques de denegación de servicio, y el uso no autorizado de los servicios, tales como-retransmisión de correo electrónico.	60 Días

Tabla 1 Tabla de severidad y tiempos de remediación para la gestión de Vulnerabilidades

La remediación de este tipo de vulnerabilidades implica el estricto cumplimiento de la política de control de cambios.

7.6 Remediación análisis de pruebas de intrusión semestrales

Las observaciones identificadas mediante las pruebas semestrales de intrusión o HE, deben ser remediadas de acuerdo con la siguiente línea de tiempo:

Severidad	Tiempo esperado de remediación
Crítica	15 días hábiles
Alta	30 días hábiles
Media	60 días hábiles
Baja	90 días hábiles

Tabla 2 Tiempos de remediación para pruebas de HE

Para las observaciones donde su remediación dependa de recursos tecnológicos que actualmente no estén disponibles, el plan de acción de remediación debe ser documentado y presentado al/la Líder de Seguridad de la Información y el/la CISO de acuerdo con la siguiente línea de tiempo.

Severidad	Tiempo esperado de remediación
Crítica	15 días hábiles
Alta	30 días hábiles
Media	60 días hábiles
Baja	90 días hábiles

Tabla 3 Tiempos de remediación y plan de acción para Vulnerabilidades detectadas en escaneos

La remediación de este tipo de vulnerabilidades implica el estricto cumplimiento del documento GINFO-POLITICA-012 LINEAMIENTOS PARA LA GESTIÓN DEL CAMBIO.

En caso de que no sea posible remediar las vulnerabilidades detectadas en los escaneos y en las pruebas de intrusión en el plazo definido, se debe documentar en el documento "INTI-F-027 PLAN DE ACCIÓN PARA REMEDIACIÓN DE VULNERABILIDADES", las razones por las cuales no se puede realizar el proceso de remediación, entre las cuales pueden identificarse: El servicio o equipo va a salir de los entornos operativos (*decomission*), renovación, actualización, propósito de almacenamiento de históricos, entre otros. Adicionalmente si se identifica que no es viable realizar la remediación y se debe asumir el riesgo, se deben documentar los activos y las razones en el acta de aceptación de riesgos, el cual debe ser aceptado por el/la subdirector/a de Sistemas de Información o quien haga las veces de CISO.

7.7 Reporte

El equipo de Seguridad de la Información reportará periódicamente a la Subdirección de Sistemas de Información el estado general de vulnerabilidades para cada Unidad Estratégica de Negocio, relacionando un análisis diferencial y comparando el estado actual con respecto al inmediatamente anterior.

Cuando se identifiquen nuevas vulnerabilidades se realizarán pruebas a los componentes tecnológicos (servidores, Bases de Datos, equipos de Comunicación y Estaciones de Trabajo) en donde se revise si se encuentran vulnerables o no.

7.8 Funcionarios y contratistas de la Agencia Nacional de Tierras

Es responsabilidad de todos los funcionarios de la Agencia Nacional de Tierras, la notificación de la identificación de vulnerabilidades en equipos, sistemas o procesos que afecten la seguridad de la información y ciberseguridad, que sean susceptibles de materializarse en cualquier activo tecnológico o de información a través de la herramienta de Mesa de Ayuda - CAS, o mediante correo electrónico a la dirección: seguridadinformatica@ant.gov.co. La notificación se hará únicamente al equipo de seguridad de la información y al líder de área de la entidad.

7.9 Notificación a terceros

La notificación de identificación, validación, cierre y excepción de vulnerabilidades de seguridad de la información y ciberseguridad, ocurridos en la infraestructura o información de los clientes, proveedores u otros terceros, se realizará a través del punto de contacto definido con el cliente o tercero. La información suministrada será la mínima que permita la identificación de la gestión y cierre de las vulnerabilidades, siempre y cuando la vulnerabilidad haya afectado activos que presten el servicio contratado con el cliente/titular/entidad y siempre asegurando la confidencialidad sobre la infraestructura, información o activos afectados y según la definición pactada a nivel contractual o legal con el tercero, a través de un certificado firmado por el/la Líder de Seguridad de la Información y el/la Jefe de Seguridad de la Información o CISO previa revisión por parte de la SSIT.

Los certificados se emitirán únicamente a los clientes/titulares/entidades si la materialización de la vulnerabilidad afecta directamente la infraestructura o información del servicio contratado y en ningún caso se reportará de forma general a terceras partes la gestión de vulnerabilidades de la entidad.

7.10 Lineamientos para el aseguramiento de plataforma

- El Equipo de Seguridad de la Información es responsable de definir mecanismos, estándares, procedimientos y/o formatos donde se establezcan los parámetros mínimos de seguridad que deben ser aplicados en los componentes tecnológicos de la Agencia Nacional de Tierras, por medio de los cuales se garantice que las vulnerabilidades propias de instalaciones por defecto, servicios inseguros, controles de acceso inadecuados, usuarios por defecto en sistemas de información, entre otros sean remediadas.
- El Equipo de Seguridad de la Información diseñará guías con configuraciones de seguridad mínimas que deben tener los dispositivos a la plataforma tecnológica de la Agencia Nacional de Tierras (Bases de datos, servidores, estaciones de trabajo y equipos de comunicaciones), tomando como referencia las configuraciones recomendadas por los proveedores de cada sistema y las guías diseñadas por CISecurity.
- Las actividades de aseguramiento/endurecimiento de plataforma tecnológica (Hardening) deben realizarse con una periodicidad anual.
- Es responsabilidad de cada administrador de los diferentes activos tecnológicos (Comunicaciones, Servidores, Bases de Datos, Estaciones de Trabajo), garantizar la aplicación de las actividades de aseguramiento teniendo en cuenta la configuración segura suministrada por el Equipo de Seguridad de la Información y las buenas prácticas de configuración y sin limitarse a ellos, basarse en la experiencia y conocimientos en aseguramiento de infraestructura de cada administrador en todos los dispositivos que hagan parte de la infraestructura tecnológica de la Agencia Nacional de Tierras antes y después de la salida a producción, asegurando siempre la transferencia de conocimiento e informando oportunamente a seguridad de la información cualquier nuevo método de aseguramiento necesario. Adicionalmente las actividades de aseguramiento deben ser realizadas con una periodicidad no mayor a un año y se debe realizar una revisión de las políticas y configuraciones periódica, la cual es definida por cada administrador de plataforma.
- En relación con las áreas críticas de la entidad es indispensable implementar siempre las instrucciones de aseguramiento explícitas en el documento: INTI-F-028 GUÍA DE ASEGURAMIENTO ESTACIONES DE TRABAJO ÁREAS CRITICAS y agregar los usuarios de estos equipos a los grupos de Hardening definidos en Directorio Activo, esta tarea se llevará acabo cada vez que ingrese un equipo de cómputo y sea asignado a estas áreas. El equipo de seguridad de la información realizará auditorías aleatorias y programadas para verificar el cumplimiento de esta directriz.
- El equipo de seguridad de la información realizará verificaciones aleatorias de validación de aplicación de las plantillas de aseguramiento, de encontrarse glosas respecto de las configuraciones, el área de Infraestructura realizará el plan de trabajo para remediarlas, en caso de que una configuración de aseguramiento genere incompatibilidades o afectaciones a un servicio, el área de infraestructura proveerá la evidencia de la misma con suficiencia técnica demostrada con pruebas de funcionamiento y procesos de los sistemas operativos y de información.

7.11 Responsabilidades

La violación, vulneración y/o cualquier infracción en todo o en parte a esta política y/o a las complementarias y/o que la adicionen, se considera falta gravísima a las obligaciones contractuales como funcionario/contratista de la Agencia Nacional de Tierras, por lo que da lugar a la terminación con justa causa de la relación laboral, comercial y/o civil.

7.12 MECANISMOS DE SEGUIMIENTO, CONTROL Y MEJORA CONTINUA

Con el propósito de garantizar la eficacia, oportunidad y consistencia del proceso de gestión de vulnerabilidades en los componentes tecnológicos y de información de la Agencia Nacional de Tierras (ANT), se establecen los siguientes mecanismos institucionales de seguimiento, control y mejora continua:

- **Seguimiento a vulnerabilidades identificadas**

  Todas las vulnerabilidades detectadas mediante escaneos, pruebas de intrusión, reportes del SOC/NOC, notificaciones internas o externas, deberán ser registradas en los sistemas de trazabilidad definidos por la Subdirección de Sistemas de Información de Tierras. Dichos sistemas deberán permitir el monitoreo, actualización y evaluación del estado de cada vulnerabilidad, incluyendo su remediación, excepción o aceptación de riesgos.

- **Indicadores de gestión de vulnerabilidades**

  La Subdirección de Sistemas de Información de Tierras, en articulación con el equipo de Seguridad de la Información, definirá indicadores que permitan medir el desempeño del proceso de gestión de vulnerabilidades. Entre ellos, se incluyen:
  - Número de vulnerabilidades detectadas por severidad (crítica, alta, media, baja).
  - Porcentaje de vulnerabilidades remediadas dentro del tiempo definido por la política.
  - Tiempos promedio de remediación.
  - Número de excepciones aprobadas por periodo.
  - Vulnerabilidades reincidentes o no remediadas.
  - Evolución de la superficie de ataque institucional.

  Estos indicadores deberán actualizarse periódicamente y socializarse a los órganos de decisión correspondientes.

- **Revisión periódica del proceso de gestión de vulnerabilidades**

  El equipo de Seguridad de la Información, con participación de las áreas técnicas responsables (infraestructura, desarrollo, arquitectura, proveedores, entre otros), realizará revisiones periódicas del proceso con el fin de:
  - Identificar cuellos de botella o retrasos recurrentes.
  - Verificar el cumplimiento de los tiempos de remediación establecidos.
  - Evaluar la efectividad de la comunicación entre actores.
  - Proponer mejoras al ciclo de identificación, análisis, priorización y remediación.

  Estas revisiones deberán realizarse, como mínimo, una vez por trimestre.

- **Gestión del conocimiento y lecciones aprendidas**

  Los aprendizajes derivados de la atención de vulnerabilidades, incidentes asociados, pruebas de intrusión o fallas de configuración deberán documentarse y compartirse con las áreas responsables. Esto permitirá fortalecer:
  - Las prácticas de seguridad.
  - La prevención de errores repetitivos.

- El diseño de mejores controles técnicos y de proceso.
- La madurez del ecosistema institucional de ciberseguridad.

Las lecciones aprendidas deberán ser incorporadas en los procedimientos, instructivos y guías asociados.

- **Inspecciones de Seguridad, Auditoría y control interno**

El proceso de gestión de vulnerabilidades será objeto de Inspecciones de Seguridad, auditorías internas y/o externas como parte del Sistema Integrado de Gestión (SIG), del MSPI, y de las auditorías institucionales o gubernamentales. Estas inspecciones/auditorías podrán verificar:

- La trazabilidad de las vulnerabilidades.
- El cumplimiento de los tiempos de remediación.
- La consistencia entre hallazgos reales y registros documentados.
- El cumplimiento de normatividad, mejores prácticas y procedimientos internos.

Las recomendaciones resultantes deberán ser incorporadas en los planes de mejora institucional.

- **Actualización de la política**

La presente política será revisada y actualizada, al menos, una vez al año o cada vez que:

- Se modifique la normatividad aplicable.
- Se presenten cambios significativos en la estructura organizacional.
- Se adopten nuevas tecnologías o modelos de arquitectura (ej. nube, contenedores, microservicios).
- Se identifiquen mejoras necesarias derivadas de auditorías, incidentes o lecciones aprendidas.

La Subdirección de Sistemas de Información de Tierras y el Equipo de Seguridad de la Información serán responsables de liderar la actualización y publicación de la política.

7.13 VIGENCIA

La presente Política de Gestión de Vulnerabilidades entra en vigor a partir de la fecha de su aprobación formal por parte de la Subdirección de Sistemas de Información de Tierras y permanecerá vigente hasta que sea modificada, actualizada o derogada expresamente mediante acto administrativo o documento de igual jerarquía.

Cualquier ajuste derivado de cambios normativos, tecnológicos, organizacionales o de mejora continua será incorporado en las versiones posteriores de esta política, las cuales deberán ser comunicadas oportunamente a todas las áreas responsables y partes interesadas.

La vigencia de esta política no exime a funcionarios, contratistas o terceros de su cumplimiento obligatorio, ni limita la aplicación de controles o procedimientos complementarios establecidos por la Agencia Nacional de Tierras o por las autoridades competentes en materia de seguridad de la información y seguridad digital.

HISTORIAL DE CAMBIOS		
Fecha	**Versión**	**Descripción**
18/12/2025	01	Primera versión del documento, creada con el objetivo de establecer los lineamientos para la gestión integral de vulnerabilidades en los activos de información, infraestructura tecnológica, aplicaciones, plataformas y servicios de la Agencia Nacional de Tierras, permitiendo identificar, evaluar, priorizar, tratar y monitorear debilidades técnicas que puedan afectar la seguridad, la continuidad operativa y la resiliencia institucional, garantizando una gestión oportuna, coordinada y trazable de los riesgos asociados.

APROBACIÓN				
	NOMBRE	**CARGO**	**FIRMA**	**FECHA**
ELABORÓ	Álvaro Javier Moreno Merchán	Contratista - Subdirección de Sistemas de Información de Tierra	**ORIGINAL FIRMADO**	15/12/2025
REVISÓ	Diana Lucía Herrera Riaño	Subdirectora de Sistemas de Información de Tierras	**ORIGINAL FIRMADO**	16/12/2025
APROBÓ	**APROBACIÓN Y PUBLICACIÓN DE LA POLÍTICA** 4° Sesión Comité Institucional de Gestión y Desempeño del 18/12/2025			18/12/2025