PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN - PESI PARA LA ANI
2025 - 2026

Tabla de Contenido

Agencia Nacional de Infraestructura
Dirección: Calle 24A # 59 - 42, Bogotá D.C., Colombia
Conmutador: (+57) 601 484 88 60
Línea Gratuita: (+57) 01 8000 410151

GLOSARIO

Activos de información: Datos y recursos valiosos para una Organización.

Brechas: Falta de cumplimiento en la seguridad de la información.

Ciberseguridad: Protección de sistemas y redes informáticas contra ataques cibernéticos.

Ciclo Deming: Ciclo de mejora continua propuesto por W. Edwards Deming.

Continuidad del negocio: Planificación para asegurar la continuidad operativa en caso de interrupciones.

Desastre tecnológico: Es cualquier evento que cause una interrupción significativa en los sistemas y servicios tecnológicos de una Organización. Estos pueden incluir fallos de hardware o software, ciberataques, errores humanos, desastres naturales o cortes de energía.

DRP: Plan de Recuperación ante Desastres.

Ethical hacking: Pruebas de seguridad informática realizadas por expertos éticos.

Gestión de identidades y accesos: Proceso de controlar y gestionar el acceso a los recursos de información.

Gobierno Digital: Uso de tecnologías digitales para mejorar la administración pública.

Hoja de ruta: Plan estratégico que define objetivos y acciones a seguir.

ISO/IEC 27001: Norma internacional para la gestión de la seguridad de la información.

Parcheo: Actualización de software para corregir errores o mejorar funcionalidades.

PESI: Plan Estratégico de Seguridad de la Información (ISO/IEC 27001:2022, 2022).

Protección de datos: Medidas para proteger la privacidad y seguridad de los datos.

SOA: Arquitectura Orientada a Servicios.

VPN: Red Privada Virtual (Virtual Private Network).

Referencias: ISO/IEC 27001:2022. (2022). *Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos*. Obtenido de ISO/IEC 27001:2022: https://www.iso.org/standard/27001?form=MG0AV3

1. Introducción

La toma de decisiones y el valor potencial de los datos en el mundo actual son claves para que la protección de la información se considere esencial para la Agencia Nacional de Infraestructura - ANI, en un mundo digital cada vez más complejo en el que la ANI se compromete a proteger la información de manera integral.

El Plan Estratégico de Seguridad de la Información - PESI, tiene como objetivo crear un marco integral que permita enfrentar los desafíos de la ciberseguridad y la protección de los datos, fomentando una cultura de seguridad al interior de la entidad.

Este Plan Estratégico, busca fortalecer la seguridad y privacidad de los datos tanto institucionales como personales, cumpliendo con la normatividad vigente.

Uno de los propósitos consiste en crear un entorno digital seguro y confiable, donde la información esté protegida de amenazas cibernéticas y en el que se respete la privacidad de los usuarios.

Para lograrlo, se deben trabajar los siguientes puntos clave:

- Cultura de seguridad: Acompañamiento a través de capacitación y concientización de los colaboradores sobre temas de seguridad informática.
- Gestión de riesgos: Identificación y gestión de los riesgos que pueden afectar los datos, con implementación de medidas preventivas y correctivas.
- Respuesta a incidentes: Establecimiento de un protocolo que permita prevenir y responder de manera exitosa ante incidentes de seguridad.
- Continuidad del negocio: Preparación anticipada para procurar al máximo la continuidad de los servicios tecnológicos, minimizando el impacto de posibles interrupciones si llegaren a presentarse.
- Identificación, clasificación y actualización del inventario de activos de la información de la ANI: Acorde al requerimiento legal y regulatorio vigente.

El PESI, alineado con estándares internacionales como ISO/IEC 27001 e ISO/IEC 27701, permitirá fortalecer la seguridad informática y construir una cultura de protección de datos dentro de la ANI.

2. Objetivos

Objetivo General

Desarrollar un Plan Estratégico de Seguridad y Privacidad de la Información que, como marco integral alineado con la naturaleza y los requerimientos del negocio, respalde la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) de la ANI, en cumplimiento de las disposiciones legales y normativas vigentes y procurando la protección de los datos y la información como los activos más valiosos de la entidad.

El Plan Estratégico se proyecta para el periodo 2025-2026 y se enfoca en:

- Aprobación del Plan propuesto.
- Fortalecimiento de la cultura y las habilidades en seguridad de la información desde el Uso y la Apropiación.
- Identificación, clasificación y actualización del inventario de activos de la información de la ANI acorde al requerimiento legal y regulatorio vigente.
- Ajuste y formalización de los riesgos de seguridad y privacidad de la información.
- Gestión de incidentes de seguridad de manera efectiva.
- Acompañamiento en la proyección del plan de continuidad del negocio.
- Determinación y priorización de los proyectos a desarrollar conforme a las capacidades existentes.
- Liderazgo en la creación del Plan de Recuperación de Desastres – DRP.

Objetivos Específicos

1. Establecer las fases del plan para desarrollar las iniciativas y proyectos de seguridad y privacidad de la información de la ANI, así como la estrategia de seguridad digital, asegurando que cada etapa esté claramente delineada y alineada con los objetivos estratégicos de la entidad.
2. Publicar el PESI conforme a lo establecido en el Decreto 612 de 2018.
3. Implementar el Modelo de Seguridad y Privacidad de la Información - MSPI de acuerdo con los requerimientos establecidos en la política de Gobierno Digital, el cual adopta las mejores prácticas y estándares internacionales.
4. Incorporar, formalizar y adoptar los lineamientos referenciados y las mejores prácticas de

seguridad en la entidad, acompañando y concientizando una cultura de seguridad y privacidad que incluya tanto a los colaboradores como a las partes interesadas.

3. Alcance

El Plan Estratégico de Seguridad y Privacidad de la Información de la ANI, se diseñó para cumplir con los controles establecidos en la norma ISO/IEC 27001:2022, la gestión de riesgos y los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) de la política de Gobierno Digital.

Este plan y su observancia a los lineamientos asociados se soportan en la directriz del Gerente del Grupo Interno de Trabajo de Tecnologías de la Información y las Telecomunicaciones – GIT TIC y es aplicable a los procesos y aspectos administrativos de la entidad. Su implementación y cumplimiento son obligatorios para todos los colaboradores, interesados y terceros que presten sus servicios o tengan algún tipo de relación con la información gestionada por la Entidad.

El documento incorpora la definición estratégica de la seguridad y privacidad de la información para la ANI, determinando y priorizando los proyectos a desarrollar conforme a las capacidades existentes.

Ahora bien, para este PESI, es pertinente abordar el concepto de Plan de Continuidad del Negocio, el cual se enfoca en mantener las operaciones esenciales del negocio en su globalidad, lo que implica la intervención en conjunto de todas las áreas en el momento en que suceda una interrupción o evento imprevisto, con el fin de dar respuesta oportuna y procurar la continuidad de las actividades, funciones críticas, servicios u operaciones.

Por otro lado, el Plan de Recuperación de Desastres (DRP), se concentra específicamente en la recuperación de la infraestructura tecnológica, los sistemas de información, los datos críticos y/o la información, después de un desastre o de un incidente disruptivo, con el fin de reanudar las operaciones en el menor tiempo posible.

En ese sentido, es fundamental tener en cuenta que ambos planes se complementan y que requieren del trabajo conjunto de todas las áreas en aras de garantizar la capacidad de reacción y recuperación de la entidad; para este Plan será prioritario que el DRP se base en el Plan de Continuidad del Negocio.

El documento contiene las definiciones para la estrategia, objetivos, marco normativo y el modelo para su planeación, definiendo la hoja de ruta de implementación; este enfoque integral asegura que la ANI esté preparada para enfrentar los desafíos actuales y futuros en materia de ciberseguridad y protección de datos, fortaleciendo así las políticas de seguridad existentes, previniendo posibles daños o pérdida de información y afianzando la cultura de seguridad de la información entre todos

los colaboradores e interesados.

4. Marco Normativo

1. **Decreto 1078 de 2015**: Este decreto consolida la normatividad aplicable al sector de Tecnologías de la Información y las Comunicaciones en Colombia, facilitando su consulta y aplicación.
   Decreto-1078-de-2015-Sector-de-Tecnologías-de-la-Información-y-las-Comunicaciones-Gestor-Normativo (funcionpublica.gov.co)

2. **Norma ISO/IEC 27001:2022**: Esta norma internacional establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI). La versión 2022 incluye actualizaciones importantes en ciberseguridad y protección de la privacidad, adaptándose a las nuevas tendencias y necesidades de seguridad.
   Seguridad de la información, ciberseguridad y protección de la privacidad. sistemas de gestión de seguridad de la información. requisitos. (icontec.org)

3. **Ley 1341 de 2009**: Según el artículo 4 de dicha ley, "En desarrollo de los principios de intervención contenidos en la Constitución Política, el Estado intervendrá en el sector las Tecnologías de la Información y las Comunicaciones para lograr los siguientes fines:
   "… 11. Promover la seguridad informática y de redes para desarrollar las Tecnologías de la Información y las Comunicaciones…"".
   Ley 1341 de 2009 - Gestor Normativo - Función Pública (funcionpublica.gov.co)

4. **Decreto 767 de 2022**: Establece los lineamientos generales de la Política de Gobierno Digital, actualizando el Decreto 1078 de 2015. La Política de Gobierno Digital busca consolidar un Estado y ciudadanos competitivos, proactivos e innovadores, generando valor público en un entorno de confianza digital.
   Decreto 767 de 2022 - Gestor Normativo - Función Pública (funcionpublica.gov.co)

5. **Artículo 2.2.9.1.1.3 del Decreto 767 de 2022**: Establece los principios de la Política de Gobierno Digital, incluyendo la Seguridad y Privacidad de la Información contemplada en la Sección 2. Este habilitador busca que los sujetos obligados desarrollen capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general,

en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.
Decreto 767 de 2022 - Gestor Normativo - Función Pública (funcionpublica.gov.co)

6. **Habilitadores Transversales de la Política de Gobierno Digital**: Estos habilitadores incluyen elementos fundamentales como la Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los componentes y el logro de los propósitos de la Política de Gobierno Digital.
Manual de Gobierno Digital (mintic.gov.co)

5. Hoja de Ruta

La hoja de ruta se basó en las brechas identificadas a través del proceso de monitoreo; en el Plan Estratégico de Tecnologías de Información – PETI se indica la importancia del desarrollo de las actividades de este Plan.

Iniciativas:

1. Activos de Información:

- Identificación, clasificación y actualización del inventario de activos de información.
- Actualización de los instrumentos de gestión de la información pública.
- Publicación de los instrumentos de gestión de la información pública.
- Establecimiento de lineamientos para el etiquetado de activos de información en medios físicos y electrónicos.
- Implementación de los lineamientos definidos para la identificación (placas) de activos de información.

2. Riesgos de Seguridad y Privacidad de la Información:

- Identificar y/o actualizar los riesgos de seguridad de la información.
- Actualizar y/o definir el tratamiento de riesgos de seguridad de la información.
- Hacer seguimiento a las medidas correctivas del tratamiento de riesgos.
- Actualizar y/o completar la declaración de aplicabilidad (SoA).
- Identificar y realizar un plan de acción de Vulnerabilidades.

3. Concientización y capacitación en Seguridad y Privacidad de la Información:

- Articular el acompañamiento para la cultura de seguridad con la estrategia de Uso y Apropiación del GIT TIC y hacer uso de los distintos medios de comunicación digital dispuestos para tal fin.
- Diseñar capacitaciones programadas en seguridad de la información y socializarlas a los colaboradores de la ANI, promoviendo buenas prácticas y una cultura de seguridad.
- Revisar la pertinencia de crear indicadores de medición de resultados del proceso de concientización en Seguridad y Privacidad de la Información.

4. Protección de Datos Personales:

- Actualizar el Registro Nacional de Bases de Datos (RNBD) ante la SIC.
- Realizar seguimiento semestral al cumplimiento de los aspectos de la política de protección de datos personales.

5. Sistema de Gestión de Seguridad de la Información:

- Revisar y actualizar, de ser procedente, la política de Seguridad y Privacidad de la Información.
- Crear y actualizar la Política de derechos de accesos privilegiados.
- Realizar seguimiento a la implementación de los controles que apliquen del MSPI y de la norma ISO 27001 v. 2022.
- Acompañar y facilitar el desarrollo de las auditorías que sean programadas.
- Realizar seguimiento a los indicadores de Seguridad de la Información y determinar la pertinencia de su formalización.
- Crear y actualizar la Política de Gestión de Identidad y acceso.
- Documentar y ejecutar la Gestión de Identidades y Accesos (IAM).
- Definir y documentar los roles y responsabilidades en materia de privacidad de la información.
- Crear y actualizar el Lineamiento de Control y Depuración de Usuarios.
- Crear y actualizar el procedimiento de acceso por Virtual Private Network - VPN.
- Crear y actualizar el documento de Gestión y comunicación de incidentes de seguridad.
- Identificar, elaborar y actualizar la matriz de riesgos de seguridad para el GIT TIC.
- Socializar y enviar para revisión de la alta dirección la política de Seguridad y Privacidad de la Información.
- Articular y formalizar bajo el ciclo Deming la documentación que proceda.
- Formalizar con la Oficina de Planeación las fases, soportes y documentos del Sistema de Gestión de Seguridad de la Información – SGSI a los que haya lugar.
- Revisar y ajustar de forma periódica los proyectos de Tecnologías de la Información - TI del PETI con base en el MSPI.
- Identificar la legislación aplicable vigente para la elaboración y presentación del normograma de Seguridad de la Información.
- Responder los requerimientos de Entes de control y externos cuando proceda.

6. Continuidad del Negocio:

- Acompañamiento en la proyección del plan de continuidad del negocio.
- Acompañamiento en la modelación de los escenarios de afectación para los servicios críticos tecnológicos de la entidad.
- Seguimiento a los planes de mejoramiento que procedan.
- Planeación, ejecución y documentación de pruebas de continuidad del negocio.
- Seguimiento a las acciones propuestas en el plan de continuidad del negocio y gestión de las acciones de mejora que llegaren a proceder.

El aspecto relacionado con la continuidad de negocio desde el GIT TIC, se enfoca en el acompañamiento al Grupo Interno de Trabajo de Planeación, en quien recae su liderazgo.

7. Seguridad Informática / Ciberseguridad:

- Ejecutar y documentar pruebas de intrusión (Ethical Hacking), estableciendo su periodicidad.
- Realizar seguimiento y documentar acciones para el cierre de brechas de las vulnerabilidades que llegaren a encontrarse.
- Crear y actualizar el instructivo de Administración de las soluciones de seguridad perimetral, solicitud de accesos, análisis de reportes y la correspondiente documentación de las propuestas de mejora que se llegaren a derivar.
- Gestionar incidentes de Ciberseguridad y establecer un plan de respuesta a éstos, con el procedimiento para su solución y comunicación.
- Construir un instrumento para el análisis de Monitoreo de alto nivel del MSPI.
- Generar recomendaciones de Seguridad con la ejecución de análisis y respuesta a las solicitudes sobre Seguridad de la Información.
- Acompañar y facilitar la gestión en las auditorías programadas y en el seguimiento de planes de mejoramiento.

8. Mejora Continua:

- Se realizará autocontrol periódico y revisiones programadas del Plan en aras de identificar oportunidades de mejora y opciones de actualización de ser procedente.

Desarrollo del pilar estratégico de Seguridad de la Información alineado al Sector y Ministerio de Transporte

- **Componente Administrativo**

1. Política de Seguridad de la Información y Ciberseguridad.
2. Políticas de Seguridad Digital Aplicadas.
   2.a. Control de acceso.
   2.b. Gestión de copias de seguridad.
   2.c. Uso de dispositivos móviles.
   2.d. Uso del correo electrónico.
3. Plan de Seguridad y Privacidad de la Información.
4. Plan de Adquisiciones de Componentes de Seguridad.
5. Sensibilización, Formación y Cultura de Seguridad Digital.
6. Actualización del Autodiagnóstico MSPI.

- **Componente Tecnológico**

1. Gestión de Riesgos.
2. Gestión de Activos de Información.
3. Gestión de Incidentes.

   - Monitoreo de activos críticos.
   - Gestión de vulnerabilidades.
   - Gestión de actualizaciones (Parcheo).
   - Seguimiento a incidentes.

6. Proyectos

- Fortalecimiento de seguridad de servicios de nube.
- Fortalecimiento de seguridad servicios On-premise.
- Modernización de políticas de seguridad de la información a implementar en servicios Web.
- Plan de tratamiento de riesgos.
- Ejecución de pruebas de Hacking ético.

Grupo Interno de Trabajo Tecnologías de la Información y las Telecomunicaciones – GIT TIC

Gerente

Hernán Darío Gutiérrez Casas

Gerente de Proyectos G2 – 09

Elaboró: Ileana Andrea Navarro Castrillón – Experto G3-5
Carlos Eduardo Flórez Jara – Contratista GIT TIC
Revisó y aprobó: Hernán Darío Gutiérrez Casas – Gerente GIT TIC