Agencia Nacional de Infraestructura

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

G.I.T DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS TELECOMUNICACIONES

Control de Versiones

Fecha	Versión	Descripción	Autor
31/01/2020	1.0	Creación del Plan	Guillermo Cadena Constratista del GIT de Tecnologías de la Información y las Telecomunicaciones
26/04/2021	2.0	Revisión y Actualización Estructura y contenido del documento	Guillermo Cadena Constratista del GIT de Tecnologías de la Información y las Telecomunicaciones
30/01/2022	3.0	Actualización del documento para formular el plan para la vigencia 2022.	Oscar Ramirez Cárdenas Constratista del GIT de Tecnologías de la Información y las Telecomunicaciones
30/01/2023	4.0	Generación de versión preliminar del plan para la vigencia 2023	Oscar Ramirez Cárdenas Constratista del GIT de Tecnologías de la Información y las Telecomunicaciones

Contenido

.

1. INTRODUCCIÓN Y CONTEXTO

Hoy en día, la información está definida como uno de los activos más valiosos y primordiales para cualquier tipo de organización, valor representado en la disponibilidad, integridad y confidencialidad de esta, lo que hace necesario que las organizaciones tengan una adecuada gestión de sus recursos y activos de información.

La defensa y protección de los activos de información es una tarea esencial para asegurar la continuidad y el desarrollo de los objetivos institucionales, así como para mantener el cumplimiento normativo y regulatorio aplicable a la entidad, además traslada confianza a las partes interesadas.

Cualquier tipo de organización independiente de su tamaño y naturaleza, debe ser consciente que la diversidad de amenazas existentes en la actualidad, atentan contra la seguridad y privacidad de la información y representan un riesgo que al materializarse no solo les puede acarrear: afectación de su imagen y reputación, costos económicos, sanciónales legales, sino que pueden afectar la continuidad y supervivencia de su actividad. Lo anterior, sumado a un entorno laboral virtual en donde cada día se hace más complejo de administrar y asegurar los activos y la información, panorama que demanda entonces que cada vez más, acciones encaminadas a que la ciberseguridad forme parte de los objetivos y planes estratégicos de las organizaciones.

Lo anterior conlleva a que los responsables de velar por la protección y seguridad de sus recursos, infraestructura e información, constantemente estén adoptando, implementando y mejorando medidas de seguridad orientadas a prevenir y/o detectar los riesgos que pueden llegar a comprometer la disponibilidad, integridad y confidencialidad de los activos de información a través de los cuales se gestiona la información de la entidad, independientemente si ésta es de carácter organizacional o personal, o si es de naturaleza pública o privada.

Dicha gestión se debe realizar de manera preventiva, es decir, a través de actividades y definiciones previamente evaluadas de acuerdo con los riesgos identificados, clasificados y valorados, de tal forma que dé lugar al adecuado tratamiento de los mismos, y es justo ahí donde cobra valor el presente documento, el cual se constituye como el plan que describirá las acciones relacionadas con la adecuada gestión de la Seguridad y Privacidad de la información en la ANI, así como con la estrategia de seguridad, de acuerdo con su contexto de función, misión, visión y la normatividad que la rige.

La AGENCIA NACIONAL DE INFRAESTRUCTURA es consciente que la protección y aseguramiento de su información es fundamental para garantizar la debida gestión y contribuir de manera

adecuada para que el país pueda desarrollar la infraestructura de transporte a través de asociaciones público-privadas, generando competitividad, bienestar y confianza, razón por la cual debe adoptar y aplicar el marco normativo de Seguridad y Privacidad de la Información que contempla políticas, límites, responsabilidades y obligaciones frente a la seguridad y privacidad de la información de la entidad.

En atención a lo anterior, la entidad asumió el reto de implementar el MSPI – Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno Digital[1], reglamentado a través del decreto 1078 de 2015, modificado por el Decreto 1008 de 2018. Este decreto en el artículo 2.2.9.1.1.3. Principios, define la seguridad de la información como principio de la Política de Gobierno Digital, de igual manera en el artículo 2.2.9.1.2.1 define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales, éstos últimos son: 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; de igual manera el 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, en el parágrafo del artículo 16 indica que (…)Las autoridades deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones. Adicionalmente la resolución 500 del 10 de Marzo del 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, incorporó el modelo de seguridad y privacidad de la información – MSPI, a la política de Gobierno Digital (MinTIC, 2021).

El presente documento contiene el plan para el establecimiento de las condiciones de seguridad informática y de la información de la ANI, el cual tomará como referencia el Modelo de Seguridad y Privacidad de la estrategia de Gobierno Digital[2][3] y la norma ISO 27001, los cuales proporcionan un marco metodológico basado en buenas prácticas para llevar a cabo la implementación del mencionado modelo de manera efectiva y adecuada.

Así mismo, este documento tiene directa relación con la política de seguridad de información la cual corresponde a la declaración general que representa la posición de la Agencia Nacional de Infraestructura frente a la necesidad de protección de su información, al igual que de la preservación de aquellos activos de información que la soportan.

[1] https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/
[2] https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf
[3] https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

2. ALCANCE

En la ANI el Modelo de Seguridad y Privacidad es de carácter transversal ya que tiene aplicabilidad a todos los procesos y aspectos administrativos de la organización y es de obligatorio cumplimiento por parte de todos aquellos servidores públicos y terceros que presten sus servicios o tengan algún tipo de relación con la información gestionada por la entidad los elementos que intervienen en su tratamiento, al efecto en los planes asociados, se contempla la protección de la información tanto en medios digitales, como no digitales.

La ANI procede a la publicación de la versión preliminar de este documento, en cumplimiento de las normas establecidas y lo actualizará en caso de ser necesario, para alinearlo a los planes del sector y de la entidad, razón por la cual este documento está sujeto a cambios.

3. ESTRATEGIA DE SEGURIDAD.

La estrategia de seguridad de la entidad en la presente vigencia 2023 se enfoca en continuar el fortalecimiento de las medidas de control que hacen parte del modelo de seguridad y privacidad, manteniendo un enfoque preventivo que articula los aspectos de tipo técnico y administrativo, así como de talento humano, para garantizar el mejoramiento continuo del proceso de seguridad.

Los controles de seguridad se materializan por medio de documentos, procesos y actividades, éstas últimas se desarrollan en forma permanente o esporádica, algunas de las cuales se relacionan a continuación:

- Identificación y gestión de riesgos de seguridad de la Información. La entidad cuenta con una matriz que identifica y valora los riesgos de seguridad de la información, así como del plan de tratamiento de riesgos definido y actualizado en cada vigencia.
- Mantenimiento de una cultura y capacitación en seguridad y prevención de riesgos de la información.
- Realización de actividades de gestión y monitoreo de herramientas que protegen la infraestructura de TI.
- Incorporación de la seguridad en proyectos de implementación y adopción de tecnologías de la información y ciclo de vida del software.
- Disposición de proceso de autenticación y segregación de funciones y responsabilidades para el uso de servicios y sistemas de información.
- Gestión de la seguridad en terceros y partes interesadas

Los controles antes mencionados se encuentran formalizados o hacen parte de documentos en la entidad algunos de los cuales son los siguientes:

- Políticas de Seguridad y Privacidad de la Información - GTEC-PT-001 versión 3.0 de mayo de 2020, documento que se constituye en la base de la pirámide del MSPI y que desarrolla

aspectos importantes como: roles y responsabilidades; capítulos 5 y 6 y políticas y directrices de protección de datos personales; capítulo 8.
- Procedimiento de tratamiento incidentes seguridad de información (GTEC-I-004 v1).
- Proceso de gestión y obtención de información de respaldo mediante el instructivo copias de seguridad de TI (GTEC-I-005- V1).
- Instructivo de Gestión de cambios de TI (GTEC-I-003 V1.0)

4. OBJETIVO ESTRATEGICO

El objetivo de este plan es minimizar la probabilidad de ocurrencia y el impacto de los riesgos que se puedan materializar, por medio del fortalecimiento de los controles contenidos en el Modelo de Seguridad y Privacidad de la Información en la Agencia Nacional de Infraestructura, en cumplimiento de las disposiciones vigentes.

Para el logro del objetivo antes mencionado, se contemplan los siguientes aspectos los cuales se detallan en proyectos a ejecutar en la vigencia, los cuales se detallan en la sección de formulación de los proyectos (ver ítem 7).

- Fortalecimiento de la arquitectura de referencia y componentes de seguridad para la infraestructura tecnológica en la nube y en sitio.
- Seguridad de la información de los usuarios finales mediante la adopción y apropiación de herramientas y esquemas de seguridad.
- Mantenimiento y renovación de licenciamiento a los componentes de procesamiento, almacenamiento, red inalambrica y plataforma de seguridad perimetral.
- Ejecución del plan de tratamiento de riesgos. Las actividades de este frente de trabajo se describen en el documento que contiene dicho plan y entre los elementos más relevantes se encuentran los siguientes:
    - Campañas de sensibilización, apropiación y prevención de riesgos de seguridad de la información dirigido a usuarios finales.
    - Actualización de parches a nivel de software base y software aplicativo para mitigación de vulnerabilidades.
    - Realización de ethical hacking en las plataformas expuestas a Internet.

5. MARCO LEGAL.

- Decreto 767 de mayo 16 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.
- Resolución 500 de marzo 10 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 y la resolución 746 del 14 de marzo del 2022 que fortalece algunos aspectos de la Resolución 500).

- Decreto 1078 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Norma NTC / ISO 27001:2013: Tecnología de la Información. Técnicas de seguridad de la información y Código de Práctica para controles de seguridad de la información
- Norma NTC/ISO 27002:2013: Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información
- Decreto 1008 de 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
- Norma NTC / ISO 31000:2009: Gestión de Riesgo, Principios y Directrices
- Guía para la administración del riesgo y el diseño de controles en entidades públicas VERSIÓN 4 del Departamento Administrativo de la Función Pública.

6. PROYECTOS VIGENCIA 2023.

El Plan de Seguridad y Privacidad de la Información además de tener un origen normativo y de optimización de la seguridad y privacidad de la información en la ANI, responde a las necesidades propias de la entidad y en conjunto se reflejan y articulan en uno de los proyectos establecidos en el Plan Estratégico de Tecnologías de la Información – PETI (P.04 – Continuidad en la implementación del plan de seguridad y privacidad de la información).

Los proyectos que conforman este plan se relacionan a continuación:

- **PS-01:** Fortalecimiento y mejora de servicios de nube
- **PS-02:** Fortalecimiento y mejora infraestructura en sitio.
- **PS-03:** Fortalecimiento y modernización de la plataforma tecnológica.
- **PS-04**: Continuar el plan de tratamiento de riesgos en la vigencia 2023.

La siguiente tabla detalla el alcance de los proyectos asociados al plan

PROYECTO	ID PROYECTO	DESCRIPCIÓN / ALCANCE.
Fortalecimiento y mejora de servicios de nube	PS-01	Este proyecto consiste en el desarrollo de actividades que permitan el fortalecimiento de la seguridad para los componentes contratados en la nube, tanto para infraestructura como para plataforma como servicio (IaaS, PaaS respectivamente), hacen parte del alcance los siguientes elementos:

PROYECTO	ID PROYECTO	DESCRIPCIÓN / ALCANCE.
		• Realización de assessment en seguridad y administración de Microsoft 365 y aplicación de recomendaciones generadas. • Implementación de Líneas Base de seguridad en directorio activo (incluye componente on premises). • Atención y gestión de alertas e incidentes en los servicios en nube y on premises. • Mejoramiento de la seguridad de la plataforma de ANIscopio en los componentes de Azure.
Fortalecimiento y mejora infraestructura en sitio.	PS-02	Este proyecto consiste en el desarrollo de actividades que permitan el fortalecimiento de la seguridad de la infraestructura on premises de la entidad, hacen parte del alcance los siguientes elementos: • Optimización y afinamiento de la Infraestructura de Seguridad Perimetral. • Ejecutar mantenimiento a elementos de la infraestructura tecnológica: ▪ Servidores. ▪ UPS ▪ PC. ▪ Solución WiFi. • Firewall.
Fortalecimiento y modernización de la plataforma tecnológica.	PS-03	Este proyecto abarca las actividades de renovación del licenciamiento y soporte de las herramientas para la infraestructura on premises, así como el servicio de seguridad para servicios en la nube, hacen parte del alcance los siguientes elementos. • Renovar el licenciamiento y soporte de Oracle para base de datos de ORFEO y SINFAD. • Gestionar e instalar el certificado digital SSL para los sitios y servicios que lo requieren. • Contratar la renovación del servicio de canal de Internet. • Contratar la renovación del licenciamiento y soporte de la plataforma de seguridad perimetral.

PROYECTO	ID PROYECTO	DESCRIPCIÓN / ALCANCE.
		• Renovar el licenciamiento de las herramientas de seguridad: Microsoft defender for endpoint (MDE) y Microsoft defender for office 365 (MDO).
Continuar el plan de tratamiento de riesgos en la vigencia 2023 –	PS-04	Este proyecto permite el cumplimiento de los requisitos de la norma ISO27001 relacionados con la identificación y gestión de riesgos y su detalle se describe en el documento "Plan de Tratamiento de Riesgos de Seguridad Información", es de anotar que este plan incluye los riesgos de seguridad digital.

7. HOJA DE RUTA.

La siguiente tabla muestra la realización de actividades en el tiempo y acorde al alcance establecido.

Nombre del Proyecto	2023											
	ene	feb	mar	abr	may	jun	jul	ago	sep	oct	nov	dic
Fortalecimiento y mejora de servicios de nube PS-01												
Realización de assessment en seguridad y administración de Microsoft 365.												
Implementación de Líneas Base de seguridad en directorio activo.												
Atención y gestión de alertas e incidentes en los servicios en nube y on premises.												
Mejoramiento de la seguridad de la plataforma de ANIscopio en los componentes de Azure.												
Fortalecimiento y mejora infraestructura en sitio. PS-02												
Optimización y afinamiento de la Infraestructura de Seguridad Perimetral. (conforme a plan que hace parte del contrato de soporte y mantenimiento).												
Ejecutar mantenimiento a elementos de la infraestructura tecnológica: Servidores, Infraestructura de												

Nombre del Proyecto	2023											
	ene	feb	mar	abr	may	jun	jul	ago	sep	oct	nov	dic
almacenamiento, UPS, PC, Solución WiFi, Firewall (segundo semestre)												
Fortalecimiento y modernización de la plataforma tecnológica. PS-03.												
Renovar el licenciamiento y soporte de Oracle para base de datos de ORFEO y SINFAD.												
Gestionar e instalar el certificado digital SSL para los sitios y servicios que lo requieren.												
Contratar la renovación del servicio de canal de Internet.												
Contratar la renovación del licenciamiento y soporte de la plataforma de seguridad perimetral.												
Renovar el licenciamiento de las herramientas de seguridad: Microsoft defender for endpoint (MDE) y Microsoft defender for office 365 (MDO).												
Continuar el plan de tratamiento de riesgos en la vigencia 2023												

8. DOCUMENTOS RELACIONADOS CON ESTE PLAN

El plan de seguridad y privacidad se apalanca y tiene como base las políticas y procedimientos relacionados con la gestión de seguridad de la información, entre los cuales tenemos los siguientes:

- Política General de Seguridad y Privacidad de la Información (GTEC-PT-001), la cual esta publicada en la página Web de la ANI y podrá ser consultada en el siguiente link: https://www.ani.gov.co/sites/default/files/sig//gico-p-001_politica_de_seguridad_y_privacidad_de_informacion_v2.pdf
- Gestión de Vulnerabilidades Técnicas (GTEC-I-001)
- Gestión de incidentes y requerimientos TI V (GTEC-P-002)
- Tratamiento incidentes seguridad de la información V1 (GTEC-I-004)

- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información - 2023

9. SOCIALIZACION DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.

El plan de Seguridad y Privacidad de la Información es aprobado con la firma y publicación del presente documento.

Los mecanismos de socialización del presente plan hacia los interesados son los siguientes:

Tipo de audiencia	Medio de socialización	Fecha planeada	Instrumento
Directivos de la entidad	Comité MIPG	Primer trimestre 2023	Presentación ejecutiva
Grupo Interno de Trabajo de Tecnologías de la Información y las Telecomunicaciones	Reunión de coordinación y seguimiento	02-2023	Presentación resumen y documento
Colaboradores Internos, Terceros y Partes Interesadas	Publicación en la página de la entidad	31-01-2023	Plan de Seguridad y Privacidad de la Información.

10. APROBACION.

Nombre	Cargo	Firma
Guillermo Gómez Gómez	Coordinador G.I.T. Tecnologías de la información y las Telecomunicaciones	
Diego Alejandro Morales Silva	Vicepresidente de Planeación Riesgos y Entorno	