Agencia Nacional de Infraestructura

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

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

ELABORÓ:	REVISÓ:	APROBÓ:
Guillermo Cadena Ronderos **Asesor G.I.T de Tecnologías de la Información y las Telecomunicaciones**	Andres Francisco Boada **Coordinador G.I.T de Tecnologías de la Información y las Telecomunicaciones**	Diego Alejandro Morales Silva **Vicepresidente de Planeación, Riesgos y Entorno.** Andrés Francisco Boada **Coordinador G.I.T de Tecnologías de la Información y las Telecomunicaciones**
FECHA: 31/01/2020	**FECHA:** 31/01/2020	**FECHA:** 31/01/2020

Contenido

2. OBJETIVO GENERAL 4
3. OBJETIVOS ESPECÍFICOS 4
4. ALCANCE 5
5. MARCO LEGAL. 5
6. DOCUMENTOS RELACIONADOS 5
7. GOBIERNO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 5
8. METODOLOGIA IMPLEMENTACION MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN . 6
8.1 Alineación Norma ISO 27001:2013 vs Ciclo de Operación 7
8.2 DESARROLLO DE LAS FASES 8
8.2.1 Fase Previa de Diagnostico del MSPI 8
8.2.2 Fase de Preparación 9
8.2.3 Fase de Implementación 9
8.2.4 Fase de Evaluación del Desempeño 11
8.2.4.1 Fase Seguimiento y Medición 11
8.2.5 Fase de Mejora del MSPI – Modelo de Seguridad y Privacidad de la información. 12

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

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 costos económicos, sanciónales legales, afectación de su imagen y reputación, sino que pueden afectar la continuidad y supervivencia del negocio. Lo anterior, sumando a un entorno tecnológico en donde cada día se hace más complejo de administrar y asegurar la información ello demanda entonces que cada vez más, las acciones encaminadas a la seguridad de la información formen parte de los objetivos y planes estratégicos de las organizaciones.

Por lo tanto, es indispensable que los responsables dentro de las organizaciones encargados 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 del negocio, independientemente si está es de carácter organizacional o personal, o de tipo 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 en donde cobra valor el presente documento, el cual se constituye como el plan que describirá las acciones relacionadas con la adecuada gestión para el aseguramiento de la Seguridad y privacidad de la información en la ANI, de acuerdo con su contexto de función, misión, visón 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 establecer un marco normativo de Seguridad y Privacidad de la Información que contemple 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], a su vez reglamentado a través del Decreto 1078 de 2015 para el sector de tecnologías de la información y comunicaciones y el Decreto 2573 de 2014 por el cual se establecen los lineamientos generales de la Estrategia en esta materia.

La ANI como parte del proceso de implementación del modelo enunciado dispondrá de dos instrumentos: i) en donde se definirá los lineamientos para la identificación y valoración de los activos de información y ii) en donde se definirá los lineamientos para la evaluación y tratamiento de los riesgos; siendo éstos el medio más eficaz de tratar, gestionar y minimizar los riesgos, considerando el impacto que éstos representan para la entidad y sus partes interesadas.

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 y la norma ISO 27001[2], 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, éste 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, por tal motivo define que:

La política General de Seguridad y Privacidad de la Información 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

2. OBJETIVO GENERAL

Establecer un Plan de Seguridad y Privacidad de la Información que apoye el establecimiento del Modelo de Seguridad y Privacidad de la Información de la Agencia Nacional de Infraestructura con la naturaleza y los requerimientos del negocio, en cumplimiento de las disposiciones legales vigentes y el aseguramiento de la información como el activo más importante de la entidad.

3. OBJETIVOS ESPECÍFICOS

- Definir las etapas del plan para establecer la estrategia de seguridad de la información de la Agencia.
- Adelantar la implementación del Modelo de Seguridad y Privacidad de la Información de la entidad de acuerdo con los requerimientos establecidos en la estrategia de Gobierno Digital.
- Establecer lineamientos para la implementación y/o adopción de mejores prácticas de seguridad en la entidad.

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

- Optimizar la gestión de la seguridad de la información al interior de la entidad.

4. ALCANCE

El Plan de Seguridad y Privacidad de la Información considera los controles de la norma NTC/ISO 27001:2013[3], el análisis de riesgos realizado a los procesos de la ANI, y los lineamientos del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno Digital. Por tanto, El plan de seguridad y privacidad de la información y lineamientos asociados como directriz de la Presidencia de la ANI, será de aplicabilidad e implementación para todos los procesos y aspectos administrativos de la organización y, de 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.

5. MARCO LEGAL.

- 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

6. DOCUMENTOS RELACIONADOS

- Políticas de Seguridad y Privacidad de la información
- Manual Políticas Específicas de Seguridad y Privacidad de la Información
- Plan de tratamiento de riesgos de seguridad de la información

7. GOBIERNO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El modelo de gobierno de la seguridad de la información se presentará a través de una estructura de directrices y lineamientos por niveles de acuerdo con el propósito de cada uno de ellos.

La estructura de directrices y lineamientos de seguridad de la información se define de la siguiente manera:

[3] https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-ISO-IEC27001.pdf

a. **Política general de seguridad de la información**: Documento de alto nivel que denota compromiso de la alta dirección con respecto a seguridad de la información; define reglas de comportamiento asociado a protección de activos de información.

b. **Políticas Tácticas de seguridad de la información**: Son exigencias particulares de apoyo a la política estratégica, manifiestan la manera en que se va a ejecutar a conseguir tienen propósito especial, es de estricto cumplimiento, que soportan los propósitos principales de la política estratégica del MSPI – Modelo de Seguridad y Privacidad de la información[4]

c. **Normas y estándares de seguridad de la información:** Todas aquellas reglas específicas orientadas para respaldar el cumplimiento de las políticas de gestión tecnológica.

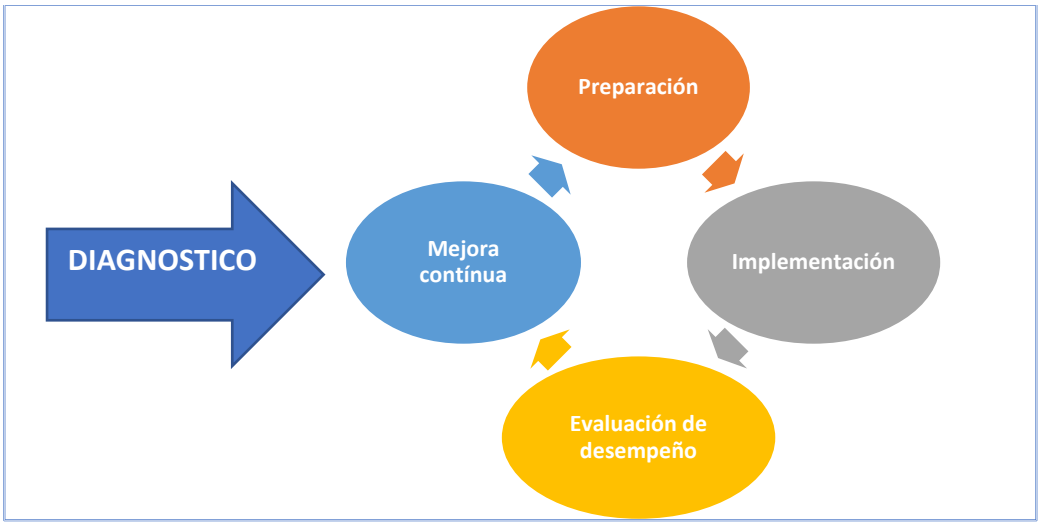
Soporte Documental: Todo documento generado para dirigir y orientar la gestión de la seguridad de la información; permitirá compartir a los servidores públicos comprender los propósitos de seguridad de la información, las directrices y lineamientos relacionados con seguridad de la información.

Toda la documentación asociada al Modelo de Seguridad y Privacidad de la información deberá ser revisada y actualizada (en la medida que aplique) bajo un estricto control de cambios para asegurar la integridad de los contenidos.

8. METODOLOGIA IMPLEMENTACION MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno Digital [5]contempla el siguiente ciclo de operación que contiene cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

[4] https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/
[5] https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf



Fase Diagnostico: Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información

- **Fase preparación:** En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos.
- **Fase Implementación (Hacer):** En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.
- **Fase Evaluación de desempeño (Verificar):** Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.
- **Fase Mejora Continua (Actuar):** Se analizan los resultados de las acciones implementadas y si estas no se cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones.

Nuevo Modelo de Ciclo de Operación del Modelo de Seguridad y Privacidad de la Información

8.1 Alineación Norma ISO 27001:2013 vs Ciclo de Operación

Aunque en la norma ISO 27001:2013 no se determina un modelo de mejora continua (PHVA) como requisito para estructurar los procesos de Seguridad de la Información, la nueva estructura de esta versión se puede alinear con el ciclo de mejora continua de las modelos de gestión de la siguiente forma:

[6]El siguiente cuadro muestra la relación entre las fases del ciclo de operación del Modelo de Seguridad y Privacidad de la Información (Diagnostico, Planificación, Implementación, Evaluación, Mejora Continua) y la estructura de capítulos y numerales de la norma ISO 27001:2013:

Fases Ciclo Operación vs Estructura ISO 27001:2013

Fase	Capitulo ISO 27001:2013
Diagnostico	4. Contexto de la Organización
Preparación	5. Liderazgos 6. Planificación 7. Soporte
Implementación	8. Operación
Evaluación de desempeño	9. Evaluación de desempeño
Mejora Continua	10. Mejora

8.2 DESARROLLO DE LAS FASES

8.2.1 Fase Previa de Diagnostico del MSPI

En esta fase y mediante el uso de herramientas de diagnóstico, se desarrollan actividades de reconocimiento y valoración del estado de gestión, cumplimento de requisitos y lineamientos de seguridad de la información basado con el Modelo de Seguridad y Privacidad de Información de la estrategia de Gobierno Digital del Gobierno Nacional[7] (u otros modelos de seguridad de la información aplicables y reconocidos), y de la implementación de controles de seguridad de la información con visión de mitigar todo tipo de escenario de riesgo asociado que pudiese generar un impacto indeseado a la Agencia.

El resultado de la evaluación de diagnóstico permitirá establecer el nivel de madurez del ciclo de operación del modelo de seguridad y privacidad de la información en la ANI, y el mapa de ruta para las actividades claves de las fases de diseño y establecimiento del mismo modelo.

[6] http://www.iso27000.es/download/doc_sgsi_all.pdf
[7] https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Actividad	Descripción	Producto	Fecha Estimada
Realizar la evaluación de diagnóstico de seguridad y privacidad de la información bajo criterios reconocidos tales como, el MSPI - Modelo de Seguridad y privacidad de la información de Gobierno Digital, al igual que bajo la ISO/IEC 27001:2013.	Obtener un informe con la identificación del estado de cumplimiento y conformidad de los aspectos de seguridad de la información de la ANI bajo el (los) modelos evaluados.	Informe de evaluación y diagnóstico del MSPI	Trimestral. 2020
Definir el mapa de ruta de las actividades orientadas a la planificación e implementación del modelo de seguridad y privacidad de la información acorde con el informe de diagnóstico.	Registro de las fases, actividades, recursos y tiempos necesarios para la planeación e implementación del modelo de seguridad y privacidad de la información.	Mapa de ruta y Cronograma de actividades	30 mayo 2020

8.2.2 Fase de Preparación

Para el desarrollo de esta fase y basado con el resultado de la evaluación de diagnóstico y el análisis de contexto de la Agencia, se identificarán los aspectos claves que definan y orienten las actividades para los propósitos de seguridad y privacidad de la información, entre ellos, la justificación, el alcance, la política y los objetivos del Modelo de Seguridad y Privacidad de la Información (MSPI).

El alcance del MSPI permitirá a la Agencia definir los límites sobre los cuales se implementará la seguridad y privacidad de la información, por tanto, deberá tener en cuenta, los procesos que impactan directamente la consecución de los objetivos misionales, procesos, servicios, sistemas de información, ubicaciones físicas, terceros relacionados e interrelaciones del MSPI con otros procesos.

8.2.3 Fase de Implementación

Permitirá a la Agencia llevar a cabo la implementación de los aspectos requisitos presentados tanto por el Modelo de Seguridad y privacidad de la información – MSPI, como los presentados por la norma ISO/IEC 27001:2013; de igual manera, la implementación de los controles de seguridad de la información, que por normativa o por resultado de la valoración de riesgos deban ser implementados.

En la fase de preparación establecerá las actividades y la programación para la implementación tanto de los requisitos, controles y buenas prácticas de seguridad y privacidad de la información en la Agencia.

Como estrategia interna para la orientación de los propósitos de seguridad y privacidad de la información, se definen e implementan políticas y directrices que guíen las prácticas de protección de la información en cuanto a su confidencialidad, integridad y disponibilidad.

A continuación, se enuncian las actividades y entregables de ésta fase:

Actividad	Descripción	Producto	Fecha Estimada
Realizar reconocimiento del contexto de la ANI (cuestiones internas y externas) con propósito de orientar el MSPI Modelo de Seguridad y Privacidad de la información como apoyo a la estrategia gerencial.	Definir los escenarios para los cuales el modelo de seguridad y privacidad de la información será soporte a la estrategia definida por la Presidencia de la ANI.	Documento con la identificación de las cuestiones internas y externas de la ANI	30 mayo 2020
Reconocer las partes interesadas de la ANI e identificar sus necesidades y expectativas con respecto a seguridad de la información	Reconocer las necesidades y expectativas de seguridad de la información por cada una de las partes interesadas de la ANI, que permitan orientar esfuerzos de cumplimiento para cada una de ellas.	Documento con la identificación de las partes interesadas, sus necesidades y expectativas pertinentes a la seguridad de información	30 junio 2020
Definir el alcance, políticas y objetivos del MSPI.	Definir el alcance y los límites bajo los servicios, procesos o actividades propias de la Agencia sobre el cual se implementará el modelo de seguridad y privacidad de la información – MSPI, la definición de la política y objetivos del MSPI.	Documento con la identificación del alcance y límites, política y objetivos del MSPI	30 agosto 2020
Definir la estructura de roles y responsabilidades para la gestión de los propósitos del MSPI y de las fases definidas	Definir y asignar formalmente la autoridad, roles y responsabilidades para la gestión y propósitos del modelo de seguridad y privacidad de información – MSPI.	Documento con la identificación y asignación de roles y responsabilidades	30 septiembre 2020
Realizar la valoración y tratamiento de los riesgos de seguridad de la información.	Definir la estrategia para identificar, estimar, evaluar y tratar los riesgos asociados a la seguridad de la información en la ANI.	Metodología para la valoración y tratamiento de los riesgos de seguridad digital	30 noviembre 2020
Definir el modelo y esquema de gestión de políticas y directrices de seguridad de la información.	Documentar el esquema de políticas y lineamientos de seguridad de la información en apoyo al cumplimiento de la política general de seguridad de la información de la ANI.	Manual de políticas específicas y lineamientos de seguridad de la información	30 noviembre 2020
Ejecutar el plan de valoración y tratamiento de los riesgos de seguridad de la información	A través de la identificación del inventario de activos de información por procesos, identificar los riesgos de seguridad de la información asociados a los mismos y aplicar la mejor estrategia de tratamiento con propósito de obtener niveles de riesgo residuales aceptables.	Inventario de activos de información	30 marzo 2021
		Mapa de riesgos de seguridad digital	
		Plan de comunicación y resultados de actividades de seguimiento al cumplimiento	30 junio 2021
Definir e implementar los controles de seguridad de la información	Implementar las estrategias de mitigación de riesgos de seguridad de la información de acuerdo con los resultados de valoración de riesgos y consecuente con los requisitos del modelo de seguridad y privacidad de la información - MSPI.	Plan de tratamiento de riesgos	30 octubre 2021

8.2.4 Fase de Evaluación del Desempeño

Con el propósito de conocer los estados de cumplimiento de los objetivos de seguridad de la información, se mantendrán esquemas de seguimiento y medición al cumplimiento de aspectos del modelo de seguridad y privacidad de información que permitan contextualizar una toma de decisiones de manera oportuna.

8.2.4.1 Fase Seguimiento y Medición

Para las actividades de seguimiento y medición, la ANI definirá procedimientos que permitan:

- Definir y orientar actividades para la identificación de situaciones de eventos o incidentes de seguridad y privacidad de la información.
- Definir los esquemas de atención a los eventos e incidentes de seguridad de la información, en beneficio de prevenir y mitigar escenarios de impacto a la Entidad.
- Emprender revisiones regulares de la eficacia del MSPI (que incluyen el cumplimiento de la política general y específicas de seguridad de la información, los objetivos, los controles) teniendo en cuenta los resultados de las auditorías de seguridad, incidentes, medición de la eficacia sugeridas y la retroalimentación de las partes interesadas.
- Medir la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad.
- Revisar las valoraciones de riesgos de manera regular, asegurando que los niveles de riesgos residuales son comprendidos y aceptados.
- Realizar ejercicios de auditoría interna del MSPI.
- Realizar actividades de revisión del MSPI por parte de la Alta Dirección de la Agencia.

Actividad	Descripción	Producto	Fecha Estimada
Definir y ejecutar la evaluación de desempeño del modelo de seguridad y privacidad de la información.	La estrategia de evaluación de desempeño establecerá el alcance y escenarios sobre los cuales se realizará seguimientos y mediciones (ejemplo, requisitos de seguridad, estados de valoración de riesgos, implementación de planes de tratamiento, etc.), los métodos elegidos, la frecuencia y los responsables de su ejecución.	Documento con la identificación y ejecución de la estrategia de evaluación de desempeño y criterios (seguimiento, medición, análisis y evaluación)	30 octubre 2021
Definir y aprobar el programa de auditoría interna del modelo de seguridad y privacidad de la información.	El programa de auditoría identificará la(s) auditoría(s) que serán realizadas para evaluar el modelo de seguridad y privacidad de la información, al igual que el cronograma para su ejecución.	Documento con la identificación del programa de auditoría	30 noviembre 2021
Realizar la revisión del estado del modelo de seguridad y privacidad de la información por parte de la alta dirección.	Recolectar las fuentes de información de aspectos del estado de operación del modelo de seguridad y	Documento de revisión por la dirección	30 noviembre 2021

Actividad	Descripción	Producto	Fecha Estimada
	privacidad de la información para presentarlas ante la alta dirección.		

8.2.5 Fase de Mejora del MSPI – Modelo de Seguridad y Privacidad de la información.

La Entidad con la visión de mantenimiento y mejora de los aspectos de seguridad de la información, tomará en cuenta los resultados de la fase III "Evaluación de desempeño" la cual está basada en los resultados de las actividades de seguimiento y medición (indicadores).

La Agencia:

- Implementará las mejoras identificadas en el MSPI
- Identificará e implementará acciones correctivas y preventivas que mitiguen situaciones de impacto.
- Implementará acciones de mejora basadas en las lecciones aprendidas de las experiencias de seguridad internas o de otras entidades.
- Velará porque las mejoras cumplen con los objetivos y propósitos definidos por la Agencia.

Actividad	Descripción	Producto	Fecha Estimada
Identificar, definir y activar planes de mejoramiento del MSPI	Los resultados y conclusiones de las actividades de evaluación de desempeño del MSPI permitirán identificar los escenarios sobre los cuales se podrán adoptar acciones correctivas o mejoras.	Plan de mejoramiento del MSPI	30 diciembre 2021