TRÁNSITO DEL ATLÁNTICO

Plan de Seguridad y Privacidad de la Información (PSPI) del Instituto de Tránsito del Atlántico para la vigencia 2025 – 2028

Oficina asesora de planeación

Departamento de Sistemas

Enero 2025

Contenido

1. Introducción y contexto general

En el contexto del mundo actual, la información representa uno de los activos más valiosos en nuestra sociedad, mucho más cuando se soporta en ellos la toma de decisiones, cualquier tipo de organización sin discriminar su tamaño y/o naturaleza debe entender su importancia, más si referenciamos el concepto actual de economías basadas e impulsadas por datos, es en este punto donde podemos tener una idea de que tan valiosos son o pueden ser.

Existen diversas amenazas físicas o digitales que atentan contra la seguridad y privacidad de la información y, representan un riesgo que si se materializa puede acarrear enormes costos económicos, sanciones legales, afectación de la imagen y reputación del Instituto, pero también, pueden significar la no continuidad y/o supervivencia del modelo de negocio afectado; todo lo anterior, sumado a un entorno tecnológico con alta complejidad en su administración y aseguramiento de la información, demandan acciones efectivas encaminadas a proteger estos recursos, para esto, es importante que estas acciones puedan ser enmarcadas en los objetivos y planes estratégicos de las organizaciones.

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 también, para mantener el cumplimiento normativo y regulatorio aplicable al Instituto, lo que al final se traduce en confianza para las partes involucradas.

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, se encarga del diseño, adopción y promoción de las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones y, es deber de todas las entidades Nacionales implementar estos lineamientos con el propósito de mitigar las posibles amenazas que puedan presentarse.

Es indispensable contar con personal capacitado al frente de la protección y seguridad de los recursos TIC dentro de las organizaciones, como también, que estos estén constantemente adoptando y/o mejorando prácticas de seguridad efectivas orientadas a prevenir los riesgos que pueden llegar a comprometer la disponibilidad, integridad y confidencialidad de los datos e información en el Instituto, esta gestión debe tener un enfoque preventivo, es decir, mediante el establecimiento previo de actividades y definiciones evaluadas, marcar la hoja de ruta a tener con el manejo de los riesgos identificados, clasificados y/o valorados, es justo aquí donde cobra valor este documento, el cual se constituye como el plan que describe las acciones relacionadas con la adecuada gestión para el aseguramiento de la Seguridad y privacidad de la información del Instituto de Tránsito del Atlántico en adelante ITA, de acuerdo con su contexto de función, misión, visón y la normatividad que lo rige.

En atención a lo anterior, ITA asumió el reto de implementar el MSPI – Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno Digital, 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.

ITA como parte del proceso de implementación del modelo enunciado, dispondrá de dos instrumentos:

- ✓ En donde se definirá los lineamientos para la identificación y valoración de los activos de información.
- ✓ En donde se definirá los lineamientos para la evaluación y tratamiento de los riesgos; considera el impacto que éstos representan para el Instituto y sus partes interesadas.

Este documento contiene el plan que establece las condiciones de seguridad informática y de la información de ITA, referenciadas en el Modelo de Seguridad y Privacidad de la estrategia de Gobierno Digital y la norma ISO 270012, los cuales proporcionan un marco metodológico basado en buenas prácticas para llevar a cabo la implementación del mencionado modelo.

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 ITA frente a la necesidad de protección de su información, como también, 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 ITA y, podrá ser consultada en el siguiente enlace: https://transitodelatlantico.gov.co/planes-de-accion-decreto-612-de-2018/

2. Objetivos

2.1. Objetivo general

Establecer un Plan de Seguridad y Privacidad de la Información que defina las directrices que ayuden a robustecer la seguridad y privacidad de la información del Instituto de Tránsito del Atlántico con la naturaleza y los requerimientos de ITA, en cumplimiento de las disposiciones legales vigentes y el aseguramiento de la información como el activo más importante del Instituto.

2.2. Objetivos específicos

- ✓ Definir las etapas del plan para establecer la estrategia de seguridad de la información del Instituto de Tránsito del Atlántico.
- ✓ Adelantar la implementación del Modelo de Seguridad y Privacidad de la Información del Instituto 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 el Instituto.
- ✓ Optimizar la gestión de la seguridad de la información al interior del Instituto.

3. Alcance

El Plan de Seguridad y Privacidad de la Información considera los controles de la norma NTC/ISO 27001:2013, el análisis de riesgos realizado a los procesos de ITA 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 alta dirección de ITA, 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 el Instituto.

4. Marco normativo

- ✓ Constitución Política de Colombia. Artículos 15, 209 y 269.
- ✓ Decreto 2106 de 2019, establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.
- ✓ Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- ✓ Decreto 1008 del 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.
- ✓ 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 ISO / IEC 27002:2013: Tecnología de la información. Técnicas de seguridad. Código de buenas prácticas para la gestión de la seguridad de la información.

5. 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.

6. 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:

Ilustración No. 1 – Estructura de Directrices y Lineamientos de Seguridad de la Información – Fuente propia

6.1. Política general de seguridad de la información

6.1.1. Definición

Es la declaración general que representa la posición del Instituto con respecto a la protección de los activos de información (funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos del Instituto y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

6.1.2. Descripción de las actividades

ITA, con el propósito de asegurar el direccionamiento estratégico establece la compatibilidad de la política y de los objetivos de seguridad de la información:

- ✓ Mitigar el riesgo de pérdida de la información del Instituto.
- ✓ Cumplir con los principios de seguridad de la información.
- ✓ Mantener la confianza de los funcionarios, contratistas y terceros.
- ✓ Apoyar la innovación tecnológica.
- ✓ Implementar el sistema de gestión de seguridad de la información.
- ✓ Proteger los activos de información.
- ✓ Definición de estándares, directrices, políticas, procedimientos e instructivos en materia de seguridad de la información.
- ✓ Fortalecer la cultura de seguridad de la información en los funcionarios y clientes externos del Instituto.
- ✓ Definir los requisitos de acceso a la información pública.
- ✓ Implementar los controles de seguridad.

6.1.3. Nivel de cumplimiento

- ✓ El Instituto ha decidido definir, implementar, operar y mejorar de forma continua un Modelo de Seguridad y Privacidad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio y a los requerimientos regulatorios que le aplican a su naturaleza.
- ✓ Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
- ✓ El Instituto protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de estos.

- ✓ El Instituto protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para esto, es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- ✓ El Instituto protegerá su información de las amenazas originadas por parte del personal.
- ✓ El Instituto protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- ✓ El Instituto controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- ✓ El Instituto implementará control de acceso a la información, sistemas y recursos de red.
- ✓ El Instituto garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- ✓ El Instituto garantizará una adecuada gestión de debilidades, eventos e incidentes de seguridad de la información asociada con los sistemas de información de la entidad.
- ✓ El Instituto garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación considerando el impacto que pueden generar los eventos.
- ✓ El Instituto garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

6.2. 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 o conseguir, tienen propósito especial, es de estricto cumplimiento y soportan los propósitos principales de la política estratégica del MSPI – Modelo de Seguridad y Privacidad de la Información

6.3. 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.

7. Metodología para la implementación del modelo de seguridad y privacidad de la información

El Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno Digital 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:

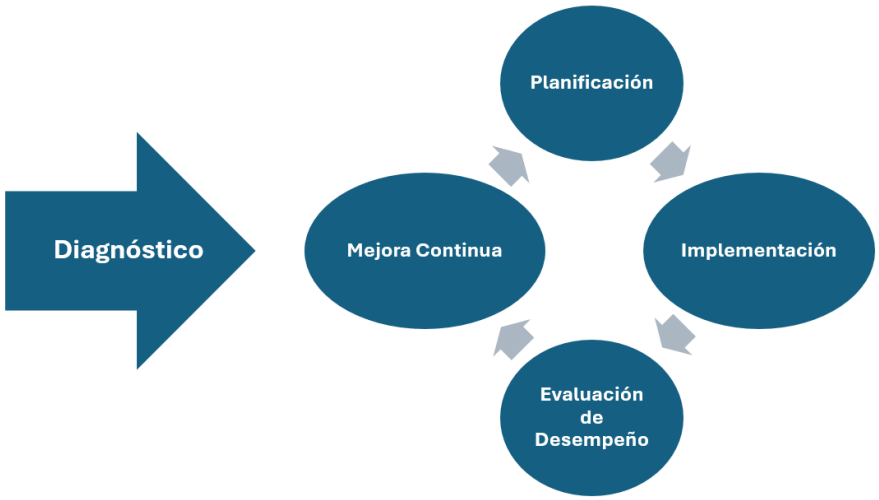

Ilustración No. 2 – Ciclo de operación del Modelo de Seguridad de Acciones y Privacidad de la Información – Fuente propia

- ✓ **Fase de diagnóstico:** se identifica el estado actual del Instituto con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.
- ✓ ***Fase de planificación:*** 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 de implementación (Hacer):*** se ejecuta el plan establecido que consiste en implementar las acciones para lograr las mejoras planteadas.
- ✓ ***Fase de 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 de 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.

7.1. Alineación de la 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 los modelos de gestión de la siguiente forma:

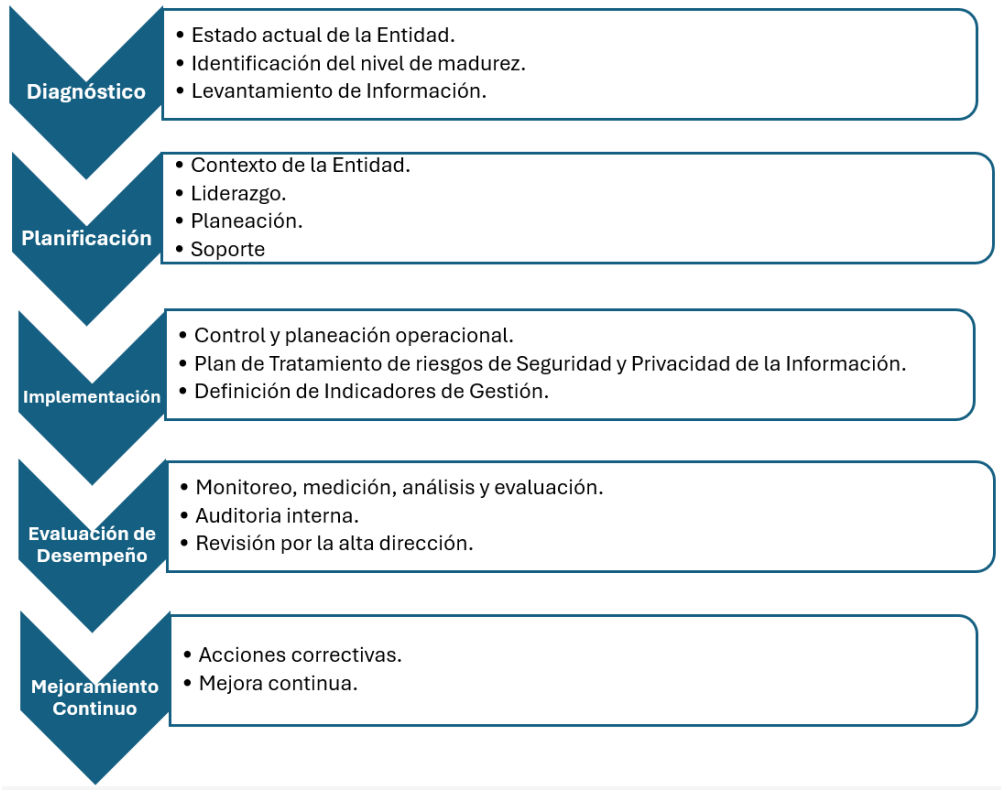

Ilustración No. 3 – Norma ISO 27001:2013 vs Ciclo de Operación.

7.2. Desarrollo de las fases

7.2.1. Fase previa de diagnóstico

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 (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 al Instituto de Tránsito del Atlántico – ITA.

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 ITA y, el mapa de ruta para las actividades claves de las fases de diseño y establecimiento del mismo modelo.

7.2.2. Fase de planificación

Para el desarrollo de esta fase y basado con el resultado de la evaluación de diagnóstico y el análisis de contexto del Instituto, 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 al Instituto 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.

7.2.3. Fase de implementación

Permitirá al Instituto 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 el Instituto.

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.

7.2.4. 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.

7.2.4.1. Fase seguimiento y medición

Para las actividades de seguimiento y medición, ITA 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 al Instituto.
- ✓ 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 del Instituto.

7.2.5. Fase de mejoramiento continuo

El Instituto 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).

El Instituto:

- ✓ 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 ITA.

7.2.6. Tabla No. 1 – Distribución de las actividades del PSPI por fases.

Fase	Actividad	Descripción	Producto	Fecha Estimada
Diagnóstico	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 Norma 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 ITA bajo el/los modelos evaluados.	Informe de evaluación y diagnóstico del MSPI.	Primer trimestre del 2025
Planificación	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.	Primer trimestre del 2025
Implementación	Realizar reconocimiento del contexto de ITA (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 Dirección de ITA.	Documento con la identificación de las cuestiones internas y externas de ITA.	Segundo trimestre del 2025
	Reconocer las partes interesadas de ITA e identificar sus necesidades y expectativas con respecto a seguridad de la información.	Reconocer las necesidades y expectativas de seguridad de la información de cada una de las partes interesadas de ITA, que permitan orientar esfuerzos de cumplimiento para cada una de estas.	Documento con la identificación de las partes interesadas, sus necesidades y expectativas pertinentes a la seguridad de información.	Segundo trimestre del 2025

	Definir el alcance, políticas y objetivos del MSPI.	Definir el alcance y los límites bajo los servicios, procesos o actividades propias del Instituto 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.	Tercer trimestre del 2025
	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.	Documento con la identificación y asignación de roles y responsabilidades.	Tercer trimestre del 2025
	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 ITA.	Metodología para la valoración y tratamiento de los riesgos de seguridad digital.	Cuarto trimestre del 2025
	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 en ITA.	Manual de políticas específicas y lineamientos de seguridad de la información.	Cuarto trimestre del 2025
	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. Mapa de riesgos de seguridad digital.	Primer trimestre del 2026
			Plan de comunicación y resultados de actividades de seguimiento al cumplimiento.	Primer trimestre del 2026

	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.	Segundo trimestre del 2026
Evaluación del desempeño - seguimiento y medición	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).	Segundo trimestre del 2026
	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.	Tercer trimestre del 2026
	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 privacidad de la información para presentarlas ante la Alta Dirección de ITA.	Documento de revisión por la Dirección ITA.	Tercer trimestre del 2026
Mejoramiento continuo	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.	Cada trimestre comprendido del cuarto trimestre 2026 al cuarto trimestre de 2028

8. Biografía

Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC. (octubre de 2021). MNGRSI – Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC. (octubre de 2021). articles-150517_Modelo_de_Seguridad_Privacidad: https://gobiernodigital.mintic.gov.co/692/articles-150517_Modelo_de_Seguridad_Privacidad.pdf

Red de Transparencia y Acceso a la Información – RTA. (diciembre de 2014) Directrices – Seguridad de la información: http://mgd.redrta.org/directrices-seguridad-de-la-informacion/mgd/2015-01-22/145337.html

9. Control de cambio

Nombre documento: PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (PSPI) DEL INSTITUTO DE TRÁNSITO DEL ATLÁNTICO PARA LA VIGENCIA 2025 – 2028.			
Código	No aplica	**Versión**	1.0
Vigencia	2025 – 2028		
Creado por	Irwing Rafael Fontalvo Nieto Profesional Universitario	**Fecha**	Enero, 2025
Revisado por	Alix Arrieta Jefe de Oficina Asesora de Planeación	**Fecha**	Enero, 2025
Aprobado por	Comité de Gestión ITA	**Fecha**	Enero, 2025

Control de Cambios	
Fecha	**Descripción**
15 de enero de 2025	Creación y elaboración de la versión 1.0 del Plan.