INPEC	GESTIÓN DE TECNOLOGÍA E INFORMACIÓN	CÓDIGO: PA-TI-PN03
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN: 6
		FECHA: 30/Ene/2025

TABLA DE CONTENIDO

Introducción

El Instituto Nacional Penitenciario y Carcelario adoptó la estrategia de Gobierno Digital como instrumento que facilita el buen gobierno y la eficiencia administrativa, eje principal que sustenta el habilitador transversal de Seguridad y Privacidad de la Política de Gobierno Digital. Este documento presenta el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

Objetivo del Plan

Actualizar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información que apoye el Sistema de Gestión de la Seguridad de la Información -SGSI - del INPEC acorde a los lineamientos del Ministerio de Tecnologías de la Información y Comunicaciones y a la Norma ISO/IEC 27001:2013 (en previsión de la publicación de la norma ISO 27001:2022, el pasado 25 de octubre del 2022, el Foro Internacional de Acreditación (IAF) ha establecido que la transición de versión de la norma en las organizaciones dispondrán de 36 meses para actualizar el SGSI) con el fin de controlar y mitigar la materialización de los riesgos asociados a la seguridad y privacidad de la información.

Objetivos Específicos

- Identificar vulnerabilidades y amenazas que dan origen al riesgo de los activos de información de las Tecnologías de la Información TI, con el propósito de prevenir la pérdida o daño de la confidencialidad, integridad y disponibilidad de los mismos en la Dirección Escuela de Formación.
- Identificar los niveles de probabilidad de ocurrencia e impacto para cada riesgo asociado a la seguridad y la privacidad de la información en la Dirección Escuela de Formación.
- Realizar monitoreo y seguimiento a los riesgos de seguridad identificados en el proceso de Gestión Tecnológica e Información, la Dirección Regional Central, Cárcel y Penitenciaria de Media Seguridad de Bogotá y Complejo Carcelario y Penitenciario con Alta Media y Mínima Seguridad de Bogotá, Cárcel y Penitenciaría con Alta y Media Seguridad Para Mujeres de Bogotá. del Instituto Nacional Penitenciario y Carcelario en virtud a lo estipulado al **PA-TI-PN03 Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información** versión oficial.

Glosario

- **Activo:** con relación con la Seguridad de la Información, se refiere a cualquier información que una organización o empresa considera importante para la misma, ya que puede estar comprendida en; Bases de datos, equipos de red, personas, infraestructura, etc.

- **Amenaza:** causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27001:2013).

- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27000).

- **Confidencialidad:** propiedad que determina que la información no esté disponible a personas no autorizados.

- **Control:** las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Disponibilidad:** propiedad de determina que la información sea accesible y utilizable por aquellas personas debidamente autorizadas

- **IAF:** Foro Internacional de Acreditación. Asociación de organismos de evaluación de acreditación y otros con interés en evaluación de la conformidad sobre sistemas de gestión, servicios, personal, productos y otros programas similares de evaluación de la conformidad

- **Impacto:** resultados y consecuencias de que se materialice un riesgo.

- **Integridad:** propiedad que busca mantener los datos libres de modificaciones no autorizadas.

- **ISO/IEC 27001:2013**: norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa.

- **Mejora Continua**: procedimiento que tiene como finalidad buscar un mayor rendimiento de los procesos o actividades

- **MSPI**: Modelo de Seguridad y Privacidad de la Información.

- **Plan de Tratamiento de Riesgos:** documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

- **Probabilidad:** medida para estimar la ocurrencia del riesgo.

- **Riesgo:** posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

- **Seguridad de la Información:** preservación de la confidencialidad, la integridad y la disponibilidad de la información.

- **SGSI Sistema de Gestión de Seguridad de la información**: permite establecer, implementar, mantener y mejorar continuamente la gestión de la seguridad de la información de acuerdo con los requisitos de la norma (ISO/IEC 27001).

- **TI**: Tecnologías de la Información.

- **Vulnerabilidad:** debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

Marco Legal

• Ver Normograma del Instituto Nacional Penitenciario y Carcelario

1. Alcance del documento

El presente Plan de Seguridad y Privacidad de la Información tiene cobertura en el proceso de Gestión Tecnología e Información y limitado a la Dirección General ubicada en la calle 26 No. 27-48, Dirección Regional Central, y los establecimientos, Complejo Carcelario y Penitenciario con Alta Media y Mínima Seguridad de Bogotá, Cárcel y Penitenciaria de Media Seguridad de Bogotá, Cárcel y Penitenciaria con Alta y Media Seguridad para Mujeres de Bogotá D.C., y Dirección Escuela de Formación conforme lo establece la **PA-TI-PL01 Política de Seguridad de la Información versión oficial**; para la presente vigencia se iniciará la fase de diagnóstico en la Dirección Escuela de Formación y se ejecutará la fase Metas y resultados de la fase de mejoramiento continuo en las demás dependencias establecidas en la política.

2. Recursos

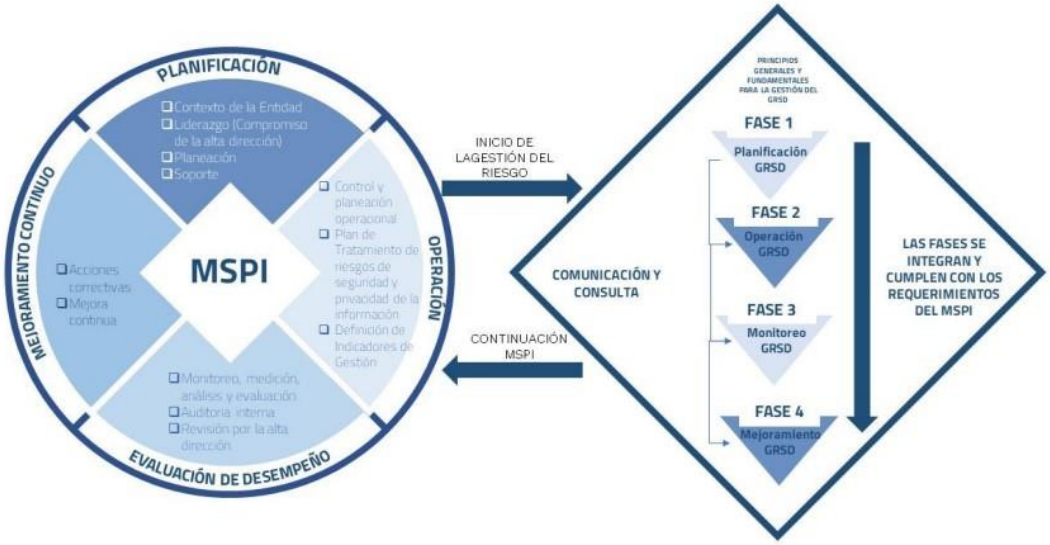
- **Humanos:** dueño de proceso, Grupo Proyección de Seguridad, e Implementación Tecnológica, servidores públicos involucrados en el proceso.
- **Tecnológico:** se dispone del correo electrónico Institucional, equipos de cómputo, canales de comunicación institucional.
- **Logístico:** reuniones presenciales y virtuales para entrevistas relacionadas con las actividades del Plan, en caso de requerirse.

3. Fases para la gestión de riesgos de seguridad de la Información

Para implementar el Modelo de Seguridad y Privacidad de la Información (MSPI) en el INPEC, se adopta el ciclo sugerido del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas (MNGRSI), complementándolo con los principios de la norma ISO/IEC 27001:2013. Este enfoque integral permitirá gestionar de manera proactiva los riesgos de seguridad de la información.

De acuerdo con esto, se definen las siguientes fases de implementación:

1. Planificación
2. Operación
3. Evaluación y seguimiento
4. Mejoramiento Continuo



FUENTE: MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Fuente: Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades publicas

3.1. Actividades del plan de tratamiento de riesgos de seguridad y privacidad de la información.

Se da a conocer las actividades del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información; lo que permite una mejora continua del Sistema de Gestión de Seguridad de la Información de la Entidad.

Actividades fase de Planificación

1. Realizar la identificación y registro de activos de información, relacionando sus respectivos dueños, clasificación y criticidad.
2. Identificar el riesgo inherente de cada activo, respecto a los tres pilares de seguridad de la información (confidencialidad, integridad y disponibilidad), asociando las posibles amenazas y vulnerabilidades que puedan causar su materialización.
3. Identificar los controles existentes y evaluar si están alineados con la norma ISO 27001:2013.
4. Definir el tratamiento adecuado para cada uno de los riesgos identificados, seleccionando alguna de las siguientes opciones: evitar, aceptar, compartir o mitigar el riesgo.

Actividades fase de operación

1. Realizar la implementación del tratamiento de riesgos definido en la fase de planificación.

2. Acompañar la implementación del plan de tratamiento de riesgos de seguridad y privacidad de la información, verificando que se ejecuten las actividades y recursos en los tiempos establecidos.

Actividades fase evaluación y seguimiento

1. Realizar registro y reporte a la Dirección Escuela de Formación, de incidentes de seguridad de la información que se hayan materializado, con el fin de identificar las causas y deficiencias en los controles aplicados.
2. Interpretar los resultados obtenidos de la evaluación de riesgos de seguridad de la información, a fin de determinar vulnerabilidades, amenazas y criticidad de los activos de información de TI en la Dirección Escuela de Formación.

Actividades fase mejoramiento continuo

1. Determinar si existen hallazgos similares en otras sedes del Instituto para tomar acciones correctivas y mitigar su materialización.
2. Revisar y evaluar los resultados obtenidos en la ejecución del Plan de Tratamiento de riesgos de seguridad y privacidad de la información, relacionados en la versión anterior, y el seguimiento a los mismos planes de vigencias anteriores, a través de la actualización de formato **PA-TI-M01-F01 Matriz de Valoración de Activos y Análisis de Riesgos de la Seguridad de la Información** versión oficial.

El monitoreo debe detectar:

- Nuevos activos o modificaciones en el valor de los activos
- Cambios o identificación de nuevas vulnerabilidades
- Nuevas amenazas
- Aumento de probabilidad de ocurrencia para cada Riesgo de la Seguridad de la Información por impacto. Lo anterior con el fin de determinar recomendaciones y controles adecuados para aceptar, disminuir, trasferir, evitar o aceptar la ocurrencia del riesgo.

ACTIVIDAD	RESULTADO	RESPONSABLE
Realizar el registro de activos de información de TI e identificación de riesgos de seguridad de la información en el Escuela Penitenciaria Nacional, bajo los lineamientos de la PA-TI-M01 Metodología de Gestión y Evaluación del Riesgo de Seguridad de la Información. Versión oficial	Levantamiento de información a través del formato PA-TI-M01-FO1 "Matriz de valoración de activos y análisis de riesgos de seguridad de la información.	Oficial de Seguridad de la Información designado por la Dirección General, con el apoyo de la Oficina de Sistemas de Información a través del Grupo Proyección Seguridad e Implementación Tecnológica, responsable del área de sistemas de la Escuela Penitenciaria Nacional, servidores públicos involucrados en el proceso
Interpretar y documentar los resultados obtenidos de la identificación y evaluación del riesgo de Seguridad de la Información en el Escuela Penitenciaria Nacional	Informe ejecutivo del análisis, interpretación y recomendaciones de la evaluación del riesgo remitido a la Dirección del Escuela Penitenciaria Nacional	Oficial de Seguridad de la Información designado por la Dirección General, con el apoyo de la Oficina de Sistemas de Información a través del Grupo Proyección Seguridad e Implementación Tecnológica.
Monitoreo y seguimiento para el proceso de Gestión Tecnológica e Información	Actualización y seguimiento de la Matriz de valoración de activos y análisis de riesgo. PA-TI-M01-FO1, versión oficial	Oficial de Seguridad de la Información designado por la Dirección General, con el apoyo de la Oficina de Sistemas de Información a través del Grupo Proyección Seguridad e Implementación Tecnológica.
Monitoreo y seguimiento para la Dirección Regional Central	Actualización y seguimiento de la Matriz de valoración de activos y análisis de riesgo. PA-TI-M01-FO1, versión oficial	Oficial de Seguridad de la Información designado por la Dirección General, con el apoyo de el encargado Área de Sistemas de la Dirección Regional Central. Apoyo Grupo Proyección Seguridad e Implementación
Monitoreo y seguimiento para la Cárcel y Penitenciaria de Media Seguridad de Bogotá	Actualización y seguimiento de la Matriz de valoración de activos y análisis de riesgo. PA-TI-M01-FO1, versión oficial	Oficial de Seguridad de la Información designado por la Dirección General, con el apoyo de el encargado Área de Sistemas de Cárcel y Penitenciaria de Media Seguridad de Bogotá. Apoyo Grupo Proyección Seguridad e Implementación Tecnológica
Monitoreo y seguimiento en el Complejo Carcelario y Penitenciario con Alta, Media y Minima seguridad de Bogota	Actualización y seguimiento de la Matriz de valoración de activos y análisis de riesgo. PA-TI-M01-FO1, versión oficial	Oficial de Seguridad de la Información designado por la Dirección General, con el apoyo de el encargado Área de Sistemas de Complejo Carcelario y Penitenciario con Alta, Media y Minima seguridad de Bogota. Apoyo Grupo Proyección Seguridad e Implementación Tecnológica
Monitoreo y seguimiento para la Cárcel y Penitenciaría con Alta y Media Seguridad Para Mujeres de Bogotá	Actualización y seguimiento de la Matriz de valoración de activos y análisis de riesgo. PA-TI-M01-FO1, versión oficial	Oficial de Seguridad de la Información designado por la Dirección General, con el apoyo de el encargado Área de Sistemas de Cárcel y Penitenciaría con Alta y Media Seguridad Para Mujeres de Bogotá con el Apoyo Grupo Proyección Seguridad e Implementación Tecnológica

4. Seguimiento al Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

El Oficial de Seguridad de la Información designado por la Dirección General, lidera el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información con el apoyo del Grupo Proyección Seguridad e Implementación Tecnológica, el área de sistemas de información y la Dirección Escuela de Formación. El seguimiento y trazabilidad de actividades se realiza a través del Plan de Acción Institucional conforme al Decreto 612 de 2018, numeral 2 del art 8 de la Resol 243 de 2020.

Anexos

• Guía No. 8 Controles de Seguridad y Privacidad de la Información. MINTIC

• PA-TI-PL01 Política de Seguridad de la Información versión oficial

• PA-TI-M01 Metodología de Gestión y Evaluación de Riesgos de Seguridad de la Información versión oficial

• PA-TI-M01-F01 Matriz de Valoración de Activos y Análisis de Riesgos de la Seguridad de la Información versión oficial

• Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades MINTIC

Lista de Versiones

Versión	Fecha de Emisión	Motivo de la Modificación	Modificaciones
1	13/Dic/2018	Creación del documento	N.A
2	29/Ene/2021	Actualización.	Cumplimiento al Decreto 612 del 2018. Aprobado mediante Acta No 001 del 26 de enero de 2021 del Comité Institucional de Gestión y Desempeño
3	18/Ene/2022	Actualización	Cumplimiento al Decreto 612 del 2018 Se actualiza el alcance el cual queda para la Cárcel y Penitenciaria de Media Seguridad de Bogotá. Se incluye monitoreo y seguimiento para la Dirección Regional Central. Aprobado mediante Acta No 01 del 12 de enero de 2022 del Comité Institucional de Gestión y Desempeño.
4	16/Feb/2023	Actualización	Cumplimiento al Decreto 612 del 2018 Se actualiza el alcance el cual queda para el Complejo Carcelario y Penitenciario con Alta Media y Mínima Seguridad de Bogotá. Se incluye monitoreo y seguimiento para la Cárcel y

			Penitenciaria de Media Seguridad de Bogotá Este documento fue Aprobado mediante Acta No. 001 del 24 de enero de 2023 del Comité Institucional de Gestión y Desempeño; se ratifica la vigencia del texto y el contenido del documento
5	29/Ene/2024	Actualización	Se realizaron las siguientes actualizaciones en el documento. 1). Actualización del Objetivo del Plan y Objetivos Específicos. 2). Inclusión en el glosario del termino "IAF". 3). Se actualizo el alcance del documento. 4). Se actualiza el contenido del titulo "3.1. Actividades del plan e tratamiento de riesgos de seguridad y privacidad de la información", para dar alcance a la Cárcel y Penitenciaría con Alta y Media Seguridad Para Mujeres de Bogotá. 5). Se incluye monitoreo y seguimiento para el Complejo Carcelario y Penitenciario con Alta Media y Mínima Seguridad de Bogotá Este documento fue Aprobado mediante Acta No. 02 del 23 de enero de 2024 en el Comité Institucional de Gestión y Desempeño.
6	17/Dic/2024	Actualización	Se realizaron las siguientes actualizaciones en el documento. 1). Actualización de los Objetivos Específicos. 2). Se actualizo el alcance del documento. 3).Se incluye monitoreo y seguimiento para la Cárcel y Penitenciaría con Alta y Media Seguridad Para Mujeres de Bogotá. 4). se adjunta en anexos el documento Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas Aprobado mediante Acta No. 04 del 24 de enero de 2025 en el Comité Institucional de Gestión y Desempeño.

Elaboró		Revisó		Aprobó	
Nombre:	Jhon Alexander Leal Mendivelso	**Nombre:**	Leonel Rios Soto	**Nombre:**	Mario Rodríguez Medina
Cargo:	Distinguido	**Cargo:**	Jefe Oficina Asesora de Planeación (E)	**Cargo:**	Jefe Oficina Sistemas de Información
Fecha:	30/Ene/2025	**Fecha:**	30/Ene/2025		

	Nombre: Laura Carolina Florez Avellaneda **Cargo:** Profesional **Fecha:** 30/Ene/2025	**Fecha:** 30/Ene/2025