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 Cárcel y Penitenciaría con Alta y Media Seguridad Para Mujeres de Bogotá.
- Identificar los niveles de probabilidad de ocurrencia e impacto para cada riesgo asociado a la seguridad y la privacidad de la información en la Cárcel y Penitenciaría con Alta y Media Seguridad Para Mujeres de Bogotá.
- Realizar monitoreo y seguimiento a los riesgos de seguridad identificados en el proceso de Gestión Tecnológica e Información, la Dirección Regional Central, la Cárcel y Penitenciaria de Media Seguridad de Bogotá y en el Complejo Carcelario y Penitenciario con Alta Media y Mínima Seguridad 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:** es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio.

- **Análisis de Riesgo:** proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

- **Confidencialidad:** es la propiedad que impide la divulgación de información a individuos, entidades o procesos no autorizados. Asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

- **Control:** cualquier actividad o acción realizada manual y/o automáticamente para prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema para conseguir sus objetivos.

- **Disponibilidad:** característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. La disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

- **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.
- **MSPI**: Modelo de Seguridad y Privacidad de la Información.
- **PHVA**: acrónimo compuesto por las iniciales de las palabras Planificar, Hacer Verificar y Actuar
- **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 la Seguridad de la Información
- **TI**: Tecnologías de la Información.
- **Valoración del riesgo**: proceso de análisis y evaluación del riesgo.
- **Vulnerabilidad:** debilidad de un activo o control que puede ser explotada por una o más amenazas.

Marco Legal

• Ver Normograma del Instituto Nacional Penitenciario y Carcelario

1. Alcance del documento

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información tiene cobertura en la Cárcel y Penitenciaría con Alta y Media Seguridad Para Mujeres de Bogotá, seguimiento en el Complejo Carcelario y Penitenciario con Alta Media y Mínima Seguridad de Bogotá, Cárcel y Penitenciaria de Media Seguridad de Bogotá, Dirección Regional Central y en el proceso de Gestión Tecnológica e Información del Instituto Nacional Penitenciario y Carcelario, como lo establece la **PA-TI-PL01 Política de Seguridad de la Información** versión oficial.

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.
- **Logístico:** reuniones presenciales y virtuales para entrevistas relacionadas con las actividades del Plan, en caso de requerirse.

3. Modelo PHVA para el SGSI

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en el INPEC, se toma como base la metodología PHVA emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC y la norma ISO/IEC 27001:2013.

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

1. Diagnosticar
2. Planear
3. Hacer
4. Actuar.

Fuente: Modelo de Seguridad y Privacidad de la Información emitida por MinTIC

3.1. Actividades del plan e 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.

1. Realizar el registro de activos que contengan información, así mismo realizar la identificación y valoración de riesgos de seguridad, basándonos en las dimensiones de confidencialidad, integridad, disponibilidad y análisis de probabilidad e impacto en la Cárcel y Penitenciaría con Alta y Media Seguridad Para Mujeres de Bogotá, acorde con lo establecido en el manual **PA-TI-M01 Metodología de Gestión y Evaluación de Riesgos de Seguridad de la Información** versión oficial y formato **PA-TI-M01-F01 Matriz de Valoración de Activos y Análisis de Riesgos de la Seguridad de la Información** versión oficial. Para ello se necesita entrevistar a los propietarios de sistemas y activos de información. "Propietario de la Información: es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso. Adaptado de ISO/IEC 27002:2013.
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 Cárcel y Penitenciaría con Alta y Media Seguridad Para Mujeres de Bogotá.
3. Tratamiento del riesgo de seguridad y privacidad de la información. Se lleva a cabo siempre después de cada evaluación de seguridad de riesgos para garantizar que se implementen controles correctos para mitigar el riesgo. Controles seleccionados del Anexo A de la norma ISO/IEC 27001:2013, o en su defecto de la Guía No. 8 "Controles de Seguridad y Privacidad de la Información" de MINTIC. ***Aunque no es una limitante se pueden seleccionar y aplicar controles diferentes a los estipulados anteriormente.***
4. Monitoreo y seguimiento. En el Complejo Carcelario y Penitenciario con Alta Media y Mínima Seguridad de Bogotá, Cárcel y Penitenciaria de Media Seguridad de Bogotá, Dirección Regional Central y proceso de Gestión de Tecnología e Información, periódicamente se revisa el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que exijan la valoración iterativa de los riesgos de seguridad de la información a través de la actualización y/o registro de la información en el formato **PA-TI-M01-F01 Matriz de Valoración de Activos y Análisis de Riesgos de la Seguridad de la Información** versión oficial. Por ello es necesario un monitoreo continuo que detecte:

    - 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 la Cárcel y Penitenciaría con Alta y Media Seguridad Para Mujeres de Bogotá, 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 Cárcel y Penitenciaría con Alta y Media Seguridad Para Mujeres de Bogotá, 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 la Cárcel y Penitenciaría con Alta y Media Seguridad Para Mujeres de Bogotá	Informe ejecutivo del análisis, interpretación y recomendaciones de la evaluación del riesgo remitido a la Dirección de la Cárcel y Penitenciaría con Alta y Media Seguridad Para Mujeres de Bogotá	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, encargado Área de Sistemas de la Dirección Regional Central. Apoyo Grupo Proyección Seguridad e Implementación Tecnológica
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, encargado del Área de Sistemas de la 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 Mínima 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, encargado del Área de Sistemas Complejo Carcelario y Penitenciario con Alta Media y Mínima Seguridad de Bogotá. 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 y la Dirección de la Cárcel y Penitenciaría con Alta y Media Seguridad Para Mujeres de Bogotá. 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

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.
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.

Elaboró	Revisó	Aprobó
Nombre: María Cristina Reyes Castillo **Cargo:** Técnico Operativo **Fecha:** 13/Dic/2023	**Nombre:** Alberto Mejía Jiménez **Cargo:** Profesional Especializado **Fecha:** 20/Dic/2023 **Nombre:** Leonel Rios Soto	**Nombre:** Adriana Cetina Hernández **Cargo:** Jefe Oficina Sistemas de Información **Fecha:** 29/Ene/2024

	Cargo:	Jefe Oficina Asesora de Planeación (E)	
	Fecha:	21/Dic/2023	

TXTCOpiaControlada