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

Establecer 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 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 TI, con el propósito de prevenir la pérdida o daño de la confidencialidad, integridad y disponibilidad de los mismos en la Dirección Regional Central.
- 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 Regional Central.
- Realizar monitoreo y seguimiento a los riesgos de seguridad identificados en el proceso de Gestión Tecnológica e Información 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 (DoS).

- **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.

- **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

- **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 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 del proceso, Grupo Proyección Seguridad, e Implementación Tecnológica, responsable de seguridad de la información designado, servidores penitenciarios involucrados en el proceso.
- **Tecnológico:** se dispone del correo electrónico institucional, equipos de cómputo, software GEPSECURE.
- **Logístico:** Reuniones presenciales y virtuales.

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 registro de activos de información de TI e identificación de riesgos de seguridad y valoración en cuanto a las dimensiones de Confidencialidad, Integridad, Disponibilidad y el análisis de probabilidad e impacto de la Dirección Regional Central, 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. "El propietario del activo puede no tener derechos de propiedad sobre el activo, pero tiene la responsabilidad de su producción, desarrollo, mantenimiento, uso y seguridad según corresponda. El propietario del activo con frecuencia es la persona más idónea para determinar el valor que el activo tiene para la organización" Fuente: NTC-ISO/IEC 27005:2009.
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 de la Dirección Regional Central.
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 los 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 la Dirección Regional Central 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.

5. Monitoreo y seguimiento para el proceso de Gestión Tecnológica e Información. Revisar y actualizar la Matriz de Valoración de Activos y Análisis de Riesgos de la Seguridad de la Información PA-TI-M01-F01 (Versión oficial) de los activos de información de TI con el objetivo de identificar nuevos impactos, amenazas, vulnerabilidades y probabilidades de riesgos de seguridad de la información, teniendo en cuenta los ítems de detección del numeral 4.

ACTIVIDAD	RESULTADO	RESPONSABLE
Realizar registro de activos de información de TI e identificación de riesgos de seguridad de la información de la Dirección Regional Central, 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-F01 V01 "Matriz de Valoración de Activos y Análisis de Riesgos de la Seguridad de la Información". Diligenciado	Oficina de Sistemas de Información en coordinación con el Grupo de Proyección Seguridad e Implementación Tecnológica, responsable de seguridad de la información designado, responsable del área sistemas de información de la Dirección de la Regional Central, servidores penitenciarios involucrados en el proceso.
Interpretar los resultados obtenidos de la evaluación del riesgo de seguridad de la Dirección Regional Central	Informe ejecutivo remitido a la Dirección Regional Central	Oficina de Sistemas de Información en coordinación con el Grupo de Proyección Seguridad e Implementación Tecnológica, responsable de seguridad de la información designado
Tratamiento del riesgo de seguridad y privacidad de la información	Informe ejecutivo remitido a la Dirección Regional Central con el resultado del tratamiento del riesgo mediante selección de controles.	Oficina de Sistemas de Información en coordinación con el Grupo de Proyección Seguridad e Implementación Tecnológica, responsable de seguridad de la información designado
Monitoreo y seguimiento en la Dirección Regional Central	Actualización y/o registro de la Matriz de Valoración de Activos y Análisis de Riesgos de la Seguridad de la Información PA-TI-M01-F01 (Versión oficial) .	Dirección Regional Central en coordinación con el responsable del área sistemas de información y apoyo del responsable de seguridad de la información designado, Grupo de Proyección Seguridad e Implementación Tecnológica
Monitoreo y seguimiento en el proceso de Gestión Tecnológica e Información	Actualización y/o registro de la Matriz de Valoración de Activos y Análisis de Riesgos de la Seguridad de la Información PA-TI-M01-F01 (Versión oficial) .	Oficina de Sistemas de Información en coordinación con el Grupo de Proyección Seguridad e Implementación Tecnológica, responsable de seguridad de la información designado

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

La Oficina de Sistemas de Información lidera el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información en coordinación con el Grupo Proyección Seguridad e Implementación Tecnológica, el responsable de seguridad de la información y la Dirección Regional Central. 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

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

Lista de Versiones

Versión	Fecha de Emisión	Motivo de la Modificación	Modificaciones
1	28/Nov/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

Elaboró	Revisó	Aprobó
Nombre: Maria Cristina Reyes Castillo	**Nombre:** Eduardo Iván Guzmán Guzmán	**Nombre:** Adriana Cetina Hernández
Cargo:	**Cargo:** Distinguido	**Cargo:** Jefe Oficina Sistemas de Información
Fecha: 29/Dic/2020	**Fecha:** 28/Ene/2021	**Fecha:** 29/Ene/2021
	Nombre: Juan Manuel Riaño Vargas	
	Cargo: Jefe Oficina Asesora de Planeación	
	Fecha: 28/Ene/2021	