TABLA DE CONTENIDO

Introducción

El Instituto Nacional Penitenciario y Carcelario adopto 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 Seguridad y Privacidad de la Información bajo el cual se espera garantizar el buen uso y protección de los activo de información.

Objetivo del Plan

Establecer el Plan 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 preservar la confidencialidad, integridad, disponibilidad y privacidad de los activos de información.

Objetivos Específicos

- Describir las actividades del Plan de Seguridad y Privacidad de la Información
- Desarrollar, verificar, aplicar y mantener la mejora continua del Sistema de Gestión de Seguridad de la Información SGSI.

Glosario

- **Activo**: en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27001:2013).

- **Activo de Información**: en relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

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

- **Análisis de riesgos**: utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.

- **Ciclo de operación**: conjunto de procesos, actividades e información que se debe realizar en cualquier tipo de organización para cumplir con el propósito para el que fue creada.

- **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

- **Dueño de proceso**: servidor penitenciario del Instituto que tiene la responsabilidad de asegurar el logro del objetivo del proceso, mediante su efectivo gerenciamiento.

- **Integridad**: propiedad de salvaguardar la exactitud y estado completo de los activos.

- **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

- **PHVA**: acrónimo compuesto por las iniciales de las palabras Planificar, Hacer Verificar y Actuar

- **Privacidad**: aspecto de la tecnología de la información (TI) que se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos en un sistema informático pueden ser compartidos con terceros.

- **Seguridad de la información**: preservación de la confidencialidad, integridad, y disponibilidad de la
información. (ISO/IEC 27001:2013).

- **Servidor Penitenciario**: es aquel funcionario que se encuentra vinculado a la planta global del INPEC ya sea por carrera administrativa, nombramiento en provisionalidad y libre nombramiento y remoción.

- **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 NTC-ISO-IEC 27001.

- **Vulnerabilidad**: debilidad de un activo o grupo de activos de información que puede ser aprovechada por una amenaza. La vulnerabilidad de caracteriza por ausencia en controles de seguridad que permite ser explotada.

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 la Dirección Regional Central como lo establece la **PA-TI-PL01 Política de Seguridad de la Información** versión oficial.

"El alcance del MSPI permite a la Entidad definir los límites sobre los cuales se implementará la seguridad y privacidad en la Entidad". Fuente: Modelo de Seguridad y Privacidad de la Información. MINTIC. Versión 3.0.2, fecha 29/07/2016.

2. Recursos

- **Humanos:** dueño de proceso, Grupo Proyección de 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, canales de comunicación.
- **Logístico**: reuniones presenciales y virtuales para la las entrevistas de identificación del nivel de madurez de la seguridad de la información.

3. Metodología implementación modelo de seguridad.

La implementación del Sistema de Gestión de Seguridad de la Información -SGSI- en la Institución, toma como referencia el Modelo de Seguridad y Privacidad de la Información -MSPI- de MINTIC donde contempla un ciclo de operación que consta de cinco (5) fases, el cual permite a la entidad gestionar adecuadamente la seguridad y privacidad de sus activos de información; así mismo toma como referencia la norma ISO/IEC 2700:2013.

3.1. Ciclo de operación

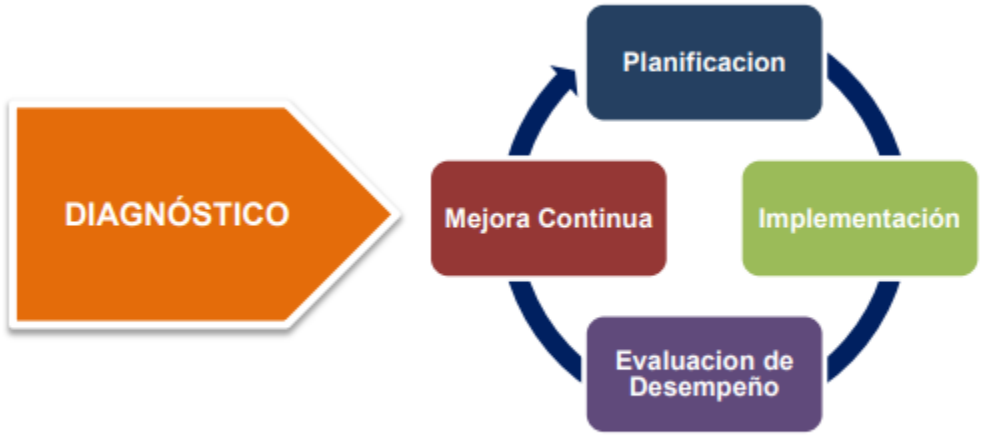

Figura 1 – Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

- **Fase de diagnóstico**: en esta fase se pretende identificar el estado actual de la Dirección Regional Central con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

Figura 2 – Etapas previas a la implementación

Fuente: Modelo de Seguridad y Privacidad de la Información. Versión 3

- **Fase de Planificación - (Planear)** : la Dirección Regional Central junto con el responsable de seguridad de la información designado debe utilizar los resultados de la etapa anterior y proceder a elaborar el plan de seguridad y privacidad de la información alineado con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.
- **Fase Implementación - (Hacer)** : esta fase le permitirá a la Dirección Regional Central, llevar acabo la implementación de la planificación realizada en la fase anterior del MSPI.

- **Fase Evaluación de Desempeño - (Verificar)**: monitoreo, análisis y evaluación de desempeño con base al seguimiento de la implementación de la seguridad de la información de la fase de implementación.
- **Fase Mejora Continua - (Actuar)**: la Dirección Regional Central con el apoyo del responsable de seguridad de la información designado debe consolidar los resultados obtenidos de la fase de evaluación de desempeño, para mejorar continuamente la seguridad y privacidad de la información, tomando oportunidades de mejora para mitigar las debilidades identificadas.

3.2. Alineación de la norma ISO/IEC 27001:2013 frente al ciclo de operación.

La norma ISO/IEC 27001:2013 determina un modelo de mejora continua (PHVA) como requisito para estructurar los procesos del Sistema de Gestión 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:

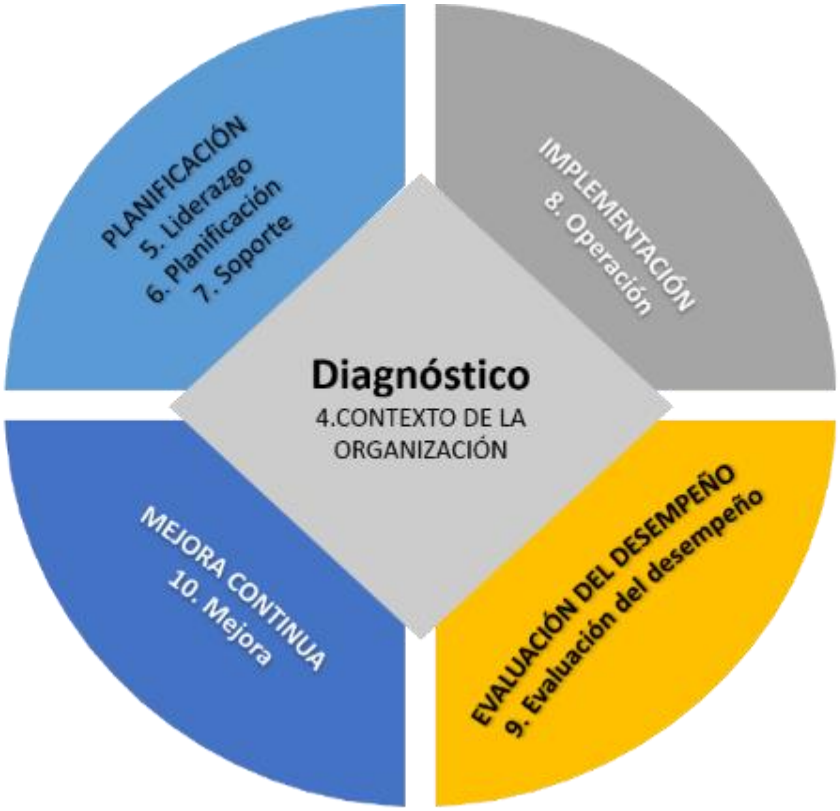

Figura: fuente propia. Alineación de la norma ISO/IEC 27001:2013 frente al ciclo de operación.

FASE MPSI	ISO 27001:2013 CAPITULO	DESCRIPCIÓN 27001:2013
Diagnóstico	4. Contexto de la Organización	Determina la necesidad de realizar un análisis de las cuestionas externas e internas de la organización y de su contexto, con el propósito de incluir las necesidades y expectativas de las partes interesadas de la organización en el alcance del SGSI.
Planeación	5. Liderazgo	Liderazgo, responsabilidades y compromiso de la alta dirección respecto al Sistema de Gestión de Seguridad de la Información asegurando una política, responsabilidades y roles pertinentes a la seguridad de la información se asignen y se comuniquen.
	6. Planificación	Define los requerimientos para la evaluación de riesgos, el tratamiento de riesgos, la declaración de aplicabilidad, el plan de tratamiento de riesgos y la determinación de los objetivos de seguridad de la información.
	7. Soporte	Define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.
Implementación	8. Operación	Indica que la organización debe planificar, implementar y controlar los procesos necesarios para cumplir los objetivos y requisitos de seguridad y llevar a cabo la valoración y tratamiento de los riesgos de la seguridad de la información. Concienciación, comunicación y control de documentos y registros.
Evaluación del desempeño	9. Evaluación del desempeño	Define los requerimientos para monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección.
Mejora continua	10. Mejora	Define los requerimientos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua.

Fuente: Norma ISO 27001:2013, página 1- 12.

4. Metas y resultados de la fases del MSPI

El Modelo de Seguridad y Privacidad de la Información contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

4.1. Metas y resultados de la fase de diagnóstico

FASE DE DIAGNÓSTICO		
META	**RESULTADO**	**RESPONSABLE**
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Dirección Regional Central	Diligenciamiento del Instrumento de Evaluación del Modelo de Seguridad y Privacidad de la Información e identificación del nivel de madurez de la entidad. creado y emitido por MINTIC	Oficina de Sistemas de Información a través del 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.
Identificar el nivel de madurez de seguridad y privacidad de la información en la Dirección Regional Central		
Identificar buenas practicas de seguridad recomendadas en PA-TI-G02 Guia de Normas y Buenas Practicas de Seguridad de la Información versión oficial a los servidores penitenciarios de la Dirección Regional Central	Informe remitido a la Dirección Regional Central y jefatura de la Oficina de Sistemas de Información	Oficina de Sistemas de Información a través del 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.

4.2. Metas y resultados de la fase de planificación

FASE DE PLANIFICACIÓN		
META	**RESULTADO**	**RESPONSABLE**
Inventario de activos de la información de las TIC (Tecnologías de la Información y la Comunicación) bajo los lineamientos de la guía PA-TI-G06 y el formato PA-TI-G06-F01 versión oficial en la Dirección Regional Central	Formato PA-TI-G06-F01 diligenciado	Oficina de Sistemas de Información a través del 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.
Concienciación de Seguridad y Privacidad de la Información a los servidores penitenciarios bajo los lineamientos del PPA-TI-PN05 Plan de sensibilización y comunicación de seguridad de la información version oficial.	Boletines de seguridad digitales, videos, charlas virtuales y/o presenciales, fondos de pantallas, pildoras de seguridad, entre otros.	Oficina de Sistemas de Información a través del Grupo de Proyección Seguridad e Implementación Tecnológica, responsable de seguridad de la información designado

4.3. Metas y resultados de la fase de implementación

FASE DE IMPLEMENTACIÓN		
META	RESULTADO	RESPONSABLE
Diseñar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información aprobado	Oficina de Sistemas de Información a través Grupo de Proyección Seguridad e Implementación Tecnológica, responsable de seguridad de la información designado
Implementación del plan de tratamiento de riesgos.	Informe de la ejecución del plan de tratamiento de riesgos remitido a la Dirección Regional Central	Oficina de Sistemas de Información a través del Grupo de Proyección Seguridad e Implementación Tecnológica, responsable de seguridad de la información designado

4.4. Metas y resultados de la fase de evaluación de desempeño

FASE EVALUACIÓN DEL DESEMPEÑO		
META	RESULTADO	RESPONSABLE
Revisión a la implementación del MSPI en la Dirección Regional Central	Informe ejecutivo	Oficina de Sistemas de Información a través del Grupo de Proyección Seguridad e Implementación Tecnológica, responsable de seguridad de la información designado

4.5. Metas y resultados de la fase de mejora

FASE MEJORA CONTINUA		
META	RESULTADO	RESPONSABLE
Analisis y recomendaciones de oportunidades de mejora para la seguridad y privacidad de la información de la Dirección Regional Central.	Informe ejecutivo	Oficina de Sistemas de Información a través del Grupo de Proyección Seguridad e Implementación Tecnológica, responsable de seguridad de la información designado
Actualización del instrumento de evaluación del MSPI de la PA-TI-PN02, V1 Política de Seguridad de la Información con el objetivo de identificar avance del nivel de madurez de la seguridad y privacidad en la Dirección General	Instrumento diligenciado	Oficina de Sistemas de Información a través del Grupo de Proyección Seguridad e Implementación Tecnológica, responsable de seguridad de la información designado servidores penitenciarios involucrados en el proceso.
Actualización de las buenas practicas sugeridas por el SGSI de la PA-TI-PN02, V1 Política de Seguridad de la Información en la Dirección General	Informe /recomendaciones	Oficina de Sistemas de Información a través del Grupo de Proyección Seguridad e Implementación Tecnológica, responsable de seguridad de la información designado servidores penitenciarios involucrados en el proceso.
Actualización del inventario de activos de información de TI en el proceso Gestión de Tecnología e información de la PA-TI-PN02, V1 Política de Seguridad de la Información, bajo los lineamientos de la guía PA-TI-G06 y el formato PA-TI-G06-F01 versión oficial	Formato PA-TI-G06-F01 diligenciado	Oficina de Sistemas de Información a través del Grupo de Proyección Seguridad e Implementación Tecnológica, responsable de seguridad de la información designado servidores penitenciarios involucrados en el proceso.

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

La Oficina de Sistemas de Información le corresponde liderar e implementar a través del Grupo Proyección de Seguridad e Implementación Tecnológica el proceso del Plan de Seguridad y Privacidad de la Información en coordinación con el responsable de seguridad de la información y la Dirección Regional Central. El seguimiento y trazabilidad de actividades se realizara 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

- Instrumento de Evaluación MSPI. MINTIC
- PA-TI-PL01 Política de Seguridad de la Información versión oficial
- PA-TI-G02 Guía de normas y buenas prácticas de la seguridad de la Información versión oficial
- PA-TI-PN05 Plan de sensibilización y comunicación de seguridad de la información versión oficial
- Modelo de Seguridad y Privacidad de la Información. MINTIC
- PA-TI-G06 Guía Inventario de activos de la información de las TIC (Tecnologías de la Información y la Comunicación) versión oficial

Lista de Versiones			
Versión	**Fecha de Emisión**	**Motivo de la Modificación**	**Modificaciones**
1	22/Nov/2018	N.A	Creación del documento.
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	