TABLA DE CONTENIDO

Introducción

La seguridad de la información identifica, valora y gestiona los activos de información y sus riesgos, buscando la protección de la información y de los sistemas de información del acceso, de utilización, divulgación o destrucción no autorizada. Los términos seguridad de la información, seguridad informática y garantía de la información tienen diferentes significados, pero todos tienen la misma finalidad que es proteger la confidencialidad, la integridad y la disponibilidad de la información sensible de la organización. Realizar correctamente la Gestión de la Seguridad de la Información requiere establecer y mantener políticas, controles y programas de seguridad.

El Instituto independiente de su complejidad y naturaleza, es consciente de la variedad de vulnerabilidades y amenazas existentes actualmente; amenazas que atentan contra la seguridad y privacidad de la información, que la protección y aseguramiento de la información es esencial para garantizar la debida gestión administrativa y operativa de la entidad.

Por lo anterior el Instituto establece el Plan de Seguridad y Privacidad de la Información, tomando como referencia los lineamientos del MINTIC y la Norma ISO/IEC 27001:2013 que contempla políticas, límites, controles, análisis de riesgos, responsabilidades y buenas prácticas frente a la Seguridad y Privacidad de la Información.

Objetivo del Plan

Establecer un Plan de Seguridad y Privacidad de la Información que apoye el Sistema de Gestión de la Seguridad de la Información -SGSI - del INPEC acorde al Modelo de Seguridad y Privacidad de la Información -MSPI - de Mintic 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

- Establecer las fases para definir la estrategia de seguridad de la información de la entidad.

- Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
- Optimizar la gestión de la seguridad de la información al interior de la entidad.
- Revisar y adoptar los roles y responsabilidades relacionados con la privacidad y seguridad de la información al interior de la entidad para optimizar su articulación.

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.
- **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
- **Integridad**: propiedad de salvaguardar la exactitud y estado completo de los activos.
- **Seguridad de la información**: preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27001:2013).
- **Sistema de Gestión de Seguridad de la información SGSI**: 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

El SGSI debe ser aplicado en los activos del Instituto, en sus las plataformas tecnológicas y en sus procesos. Este enfoque se realizara paulatinamente por procesos y luego se extenderá a toda la Entidad.

2. Recursos

- **Humanos:** líder del proceso, coordinador y personal del grupo Proyección Seguridad, e Implementación Tecnológica de la Oficina de Sistemas de Información.
- **Físicos:** Infraestructura tecnológica.
- **Financieros:** actualmente la Oficina de Sistemas de Información no cuenta con recursos financieros asignadas para el SGSI, se debe analizar y solicitar los recursos financieros necesarios para alcanzar el estado deseado en materia de seguridad de la información para implementar controles técnicos, físicos o administrativos, conforme a los resultados de una evaluación de riesgos.

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

Contienen objetivos, metas y herramientas (guías) que permiten que la seguridad y privacidad de la información sea un sistema de gestión sostenible dentro de la entidad.

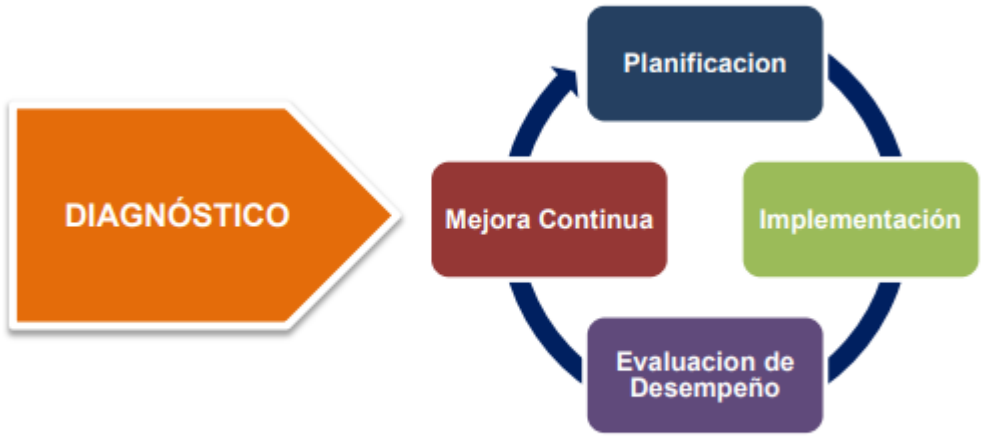

Figura 1 – Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

- **Fase de diagnóstico**: en esta fase se pretende identificar el estado actual de la entidad 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 entidad 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.

  El alcance del MSPI permite a la Entidad definir los límites sobre los cuales se implementará la Seguridad y Privacidad de la Información. Este enfoque es por procesos y debe extenderse a toda la Entidad.

- **Fase Implementación - (Hacer)**: esta fase le permitirá a la entidad, 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 entidad debe consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

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

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

La norma ISO/IEC 27001:2013 no se 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:

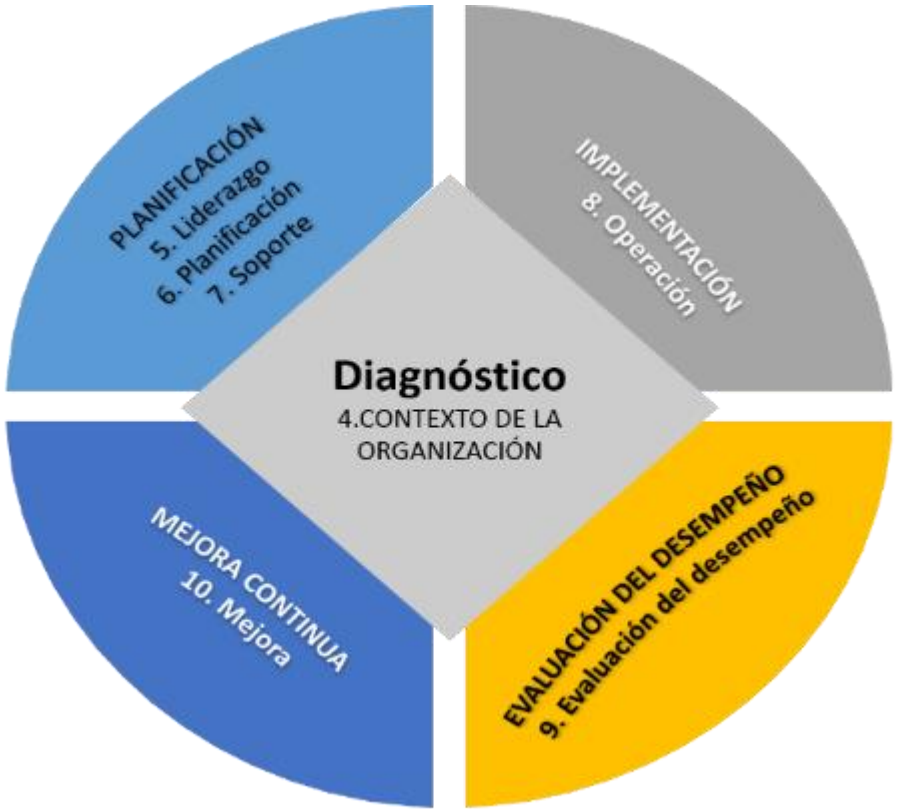

Figura: fuente propia. Alineación de la norma ISO/IEC 27001:2013 frente al ciclo de operación.

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

3.3 Metas y resultados de la fase de diagnóstico

FASE DE DIAGNÓSTICO			
META	**RESULTADO**	**TIEMPO ESTIMADO**	**RESPONSABLE**
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior del instituto	Diligenciamiento de la herramienta: Instrumento de Evaluación de Seguridad y Privacidad de la Información - MSPI- emitido por MINTIC	Febrero - Abril de 2019	Oficial de Seguridad de la Información, Grupo Proyección, Seguridad e Implementación Tecnológica de la Oficina de Sistemas de Información,
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad.			
Identificar buenas prácticas sugeridas por el SGSI.	Informe/Recomendaciones	Mayo - Junio de 2019	Oficial de Seguridad de la Información, Oficina Asesora de Planeación, Subdirección de Talento Humano, Grupo de contratación de la Subdirección de Gestión Contractual, Grupo logístico, Grupo de manejo, bienes e inmuebles Grupo de Gestión Documental de la Dirección Gestión Corporativa, Grupo Proyección, Seguridad e Implementación Tecnología de la Oficina de Sistemas de Información,

3.4 Metas y resultados de la fase de planificación.

FASE PLANEACIÓN			
META	Resultado	Tiempo estimado	Responsable
Actualizar Política de Seguridad y Privacidad de la Información e integrarla con la guía de normas y buenas prácticas de la seguridad de la Información.	Política de Seguridad de la Información actualizada e integrada con la guía de normas y buenas prácticas de la seguridad de la Información aprobado por la alta Dirección .	Febrero a Noviembre de 2019	Dirección General, Oficial de Seguridad de la Información, Oficina Asesora de Planeación, Grupo Proyección, Seguridad e Implementación Tecnológica de la Oficina de Sistemas de Información.
Roles y responsabilidades de seguridad y privacidad de la información.	Acto administrativo a través del cual se asignan los roles y responsabilidades de seguridad y privacidad de la información al interior de lña Entidad, revisado y aprobado por la alta Dirección,	Febrero a Noviembre de 2019	Dirección General, Oficial de Seguridad de la Información, Oficina Asesora de Planeación, Grupo Proyección, Seguridad e Implementación Tecnológica de la Oficina de Sistemas de Información.
Inventario de activos de de información	*Documento guía para identificación, clasificación y valoración de activos de información, revisado y aprobado por la alta dirección para luego implementarlo en el proceso Gestión de Tecnología e Información. Tomando como referencia Guía No 5 - Gestión De Activos de MINTIC. * Matriz con la identificación, valoración y clasificación de activos de información.	Junio a Noviembre de 2019	Dirección General, Oficial de Seguridad de la Información, Oficina Asesora de Planeación, Grupo Proyección, Seguridad e Implementación Tecnológica de la Oficina de Sistemas de Información, Grupo de Gestión Documental de la Dirección Gestión Corporativa.
Plan de Comunicaciones de Seguridad de la Información.	Documento con el plan de comunicación, sensibilización y capacitación para la entidad.	Octubre - Noviembre de 2019	Dirección General, Oficial de Seguridad de la Información, Escuela Penitenciaria Nacional, Oficina Asesora de Comunicaciones, Oficina Asesora de Planeación, Grupo Proyección, Seguridad e Implementación Tecnológica de la Oficina de Sistemas de Información

3.5 Metas y resultados de la fase de implementación

FASE IMPLEMENTACIÓN			
META	**Resultado**	**Tiempo estimado**	**Responsable**
Diseñar del plan de tratamiento de riesgos de seguridad de la información	Plan de tratamiento de riesgos de seguridad de la información aprobado.	Febrero - Marzo de 2019	Oficial de Seguridad de la Información, Oficina Asesora de Planeación, Grupo Proyección, Seguridad e Implementación Tecnológica de la Oficina de Sistemas de Información.
Inventario de activos de IPv6 de la Sede central.	Inventario	Febrero - Junio de 2019	Grupo de Administración de las Tecnologías de la Información de la Oficina de Sistemas de Información.
Transición de IPv4 a IPv6	Implemetación de transición del procotocolo IPV6 en coexistencia a IPV4	Febrero - Noviembre de 2019	Oficial de Seguridad de la Información, Grupo de Administración de las Tecnologías de la Información de la Oficina de Sistemas de Información.
Sensibilización y/o concienciación de Seguridad y Privacidad de la Información.	Actas de asistencia, encuestas, formularios de evaluación.	Junio a Octubre de 2019	Oficial de Seguridad de la Información, Escuela Penitenciaria Nacional, Oficina Asesora de Comunicaciones, Grupo Proyección, Seguridad e Implementación Tecnológica de la Oficina de Sistemas de Información,

3.6 Metas y resultados de la fase de evaluación de desempeño

FASE EVALUCIÓN DEL DESEMPEÑO			
META	**Resultado**	**Tiempo estimado**	**Responsable**
Revisión del diseño del Modelo MSPI.	Documento o informe ejecutivo del seguimiento y revisión del MSPI.	Noviembre - Diciembre de 2019	Oficial de Seguridad de la Información, Grupo Proyección, Seguridad e Implementación Tecnologica de la Oficina de Sistemas de Información.

3.7 Metas y resultados de la fase de mejora.

FASE MEJORA CONTINUA			
META	**Resultado**	**Tiempo estimado**	**Responsable**
Analisis de mejora para las fases de la metodología de implementación del MSPI	Documento o informe ejecutivo	Junio - Diciembre 2020	Oficial de Seguridad de la Información, Grupo Proyección, Seguridad e Implementación Tecnologica de la Oficina de Sistemas de Información.

Bibliografía.

- Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia MINITC. Modelo de Seguridad y Privacidad de la Información. Versión 3.0.2. Julio 27 de 2016.
- Norma Técnica NTC-ISO-IEC Colombiana 27001:2013.

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

Elaboró	Revisó	Aprobó
Nombre: Maria Cristina Reyes Castillo **Cargo:** Auxiliar Adminstrativo **Fecha:** 22/Nov/2018	**Nombre:** Angelica María Patiño García **Cargo:** Profesional Especializado **Fecha:** 23/Nov/2018 **Nombre:** Juan Manuel Riaño Vargas **Cargo:** Jefe Oficina Asesora de Planeación **Fecha:** 23/Nov/2018	**Nombre:** Adriana Cetina Hernández **Cargo:** Jefe Oficina Sistemas de Información **Fecha:** 23/Nov/2018