TABLA DE CONTENIDO

Objetivo del Plan
Objetivos Específicos
Glosario
Marco Legal
1.Alcance del documento
2.Recursos
3.Modelo PHVA para el SGSI
3.1. Actividades del plan e tratamiento de riesgos de seguridad y privacidad de la información.
3. 1. 1. Cronograma de actividades.
4.Entregables
Anexos

INTRODUCCIÓN

En el marco del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC y la norma técnica ISO/IEC 27005:2009 (es un soporte a la norma ISO/IEC 27001 la cual proporciona directrices para la gestión de riesgos de seguridad de la información, es aplicable a todos los tipos de organización y no proporciona ni recomienda una metodología específica). El Instituto Nacional Penitenciario y Carcelario busca prevenir impactos no deseados que se puedan presentar en cuanto a seguridad de la información, garantizando el tratamiento de los riesgos de seguridad de la información y la gestión de riesgo oportuna y objetivamente, acorde con lo establecido en la Metodología de Gestión y Evaluación de Riesgos de Seguridad de la Información PA-TI-M01 (Versión oficial) y el formato Matriz de Valoración de Activos y Análisis de Riesgos de la Seguridad de la Información PA-TI-M01-F01 F01 (Versión oficial) , para el levantamiento de información y análisis de la misma.

Objetivo del Plan

Definir el plan de tratamiento de riesgos de seguridad de la información que hace parte del Sistema de Gestión de Seguridad de la Información, para gestionar, controlar y reducir los riesgos

asociados al proceso de Gestión Tecnológica e Información, con el fin de proteger los activos de información, el manejo de medios, control de acceso y gestión de usuarios.

Objetivos Específicos

- Realizar el plan de actividades específico validando recursos con los que cuenta actualmente el INPEC, para implementar el plan de tratamiento de riesgo de seguridad y privacidad de la información.
- Aplicar la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, respectivamente en seguridad y riesgo de la información.

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.
- **Evento de Seguridad de la Información:** identificación del estado de un sistema, servicio o red, que indica una posible violación de la Política de Seguridad de la Información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.
- **Impacto:** resultados y consecuencias de que se materialice un riesgo.
- **Integridad:** propiedad que busca mantener los datos libres de modificaciones no autorizadas.

- **ISO/IEC 27005:2009:** es el estándar internacional que se ocupa de la gestión de riesgos de seguridad de información. La norma suministra las directrices para la gestión de riesgos de seguridad de la información en una empresa, apoyando particularmente los requisitos del sistema de gestión de seguridad de la información definidos en ISO 27001.
- **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.
- **PHVA:** es una estrategia de mejora continua de la calidad en cuatro pasos (Planificar, Hacer Verificar y Actuar).
- **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.
- **Riesgo residual:** riesgo que permanece tras el tratamiento del riesgo.
- **Seguridad de la Información:** preservación de la confidencialidad, la integridad y la disponibilidad de la información.

- **Sistema de Gestión de la Seguridad de la Información (SGSI):** conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de Seguridad de la Información y alcanzar dichos objetivos, basándose en un enfoque de Gestión del Riesgo y de mejora continua.
- **Tratamiento:** cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
- **Tratamiento de riesgos:** proceso de modificar el riesgo, mediante la implementación de controles.
- **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

Se define el alcance del presente plan de tratamiento de riesgos de seguridad y privacidad de la información, para el proceso de Gestión Tecnológica e Información del Instituto Nacional Penitenciario y Carcelario.

2. Recursos

- **Humanos:** líder del proceso, coordinador y personal del Grupo de Proyección, Seguridad e Implementación Tecnológica de la Oficina de Sistemas de Información.
- **Físicos:** infraestructura tecnológica.
- **Financieros:** actualmente la Oficina de Sistemas de Información cuenta con recursos financieros para el SGSI, estos recursos provienen del Proyecto de Inversión Tecnológico.

  Sin embargo es necesario gestionar más recursos para garantizar la implementación del SGSI para su permanencia y vigencia a nivel nacional.

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 (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.

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

1. Diagnosticar.
2. Planear.
3. Hacer.
4. Verificar.
5. 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 definidas del plan de tratamiento de riesgos de seguridad y privacidad de la información, con el fin de realizar el proceso concerniente a los riesgos de seguridad de la información, lo que permite una mejora continua del Sistema de Gestión de Seguridad de la Información de la Entidad:

1. Realizar diagnóstico con el fin identificar el estado actual del proceso de Gestión Tecnológica e Información con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

2. Revisar el Plan de tratamiento de riesgos de seguridad y privacidad de la información aprobado para su ejecución.

3. Realizar la identificación de los riesgos y el registro de activos de información, su valoración en cuanto a las dimensiones de Confidencialidad, Integridad, Disponibilidad y el análisis de probabilidad e impacto de los riesgos del proceso de Gestión Tecnológica e Información , acorde con lo establecido en la Metodología de Gestión y Evaluación de Riesgos de Seguridad de la Información PA-TI-M01 (Versión oficial) y el formato Matriz de Valoración de Activos y Análisis de Riesgos de la Seguridad de la Información PA-TI-M01-F01 (Versión oficial). Para ello se necesita entrevistar al líder del proceso, y 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.*

4. Interpretar los resultados obtenidos del análisis del riesgo, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

5. Seguimiento y control. Al finalizar cada etapa se realizará una reunión con el líder del proceso de Gestión Tecnológica e Información y el coordinador del grupo de Proyección, Seguridad e Implementación Tecnológica para presentar el informe del avance del proyecto y de esta manera evaluar los pasos realizados.

3. 1. 1. Cronograma de actividades.

CRONOGRAMA ACTIVIDADES PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
NOMBRE ACTIVIDAD	TIEMPO ESTIMADO	RESPONSABLE
1. Realizar diagnóstico.	Febrero-Marzo de 2019	Oficial de Seguridad de la Información , Grupo Proyección, Seguridad e Implementación Tecnologíca con el apoyo del líder del proceso Gestión de Tecnología e Información, coordinadores de los Grupos Administración de la Información , Administración de las Tecnologías de la Información, Apoyo Seguridad Electrónica.
2. Revisar el Plan de tratamiento de riesgos de seguridad y privacidad de la información aprobado para su ejecución.	Abril de 2019	Oficial de Seguridad de la Información, Líder del proceso de Gestión Tecnológica e Información, Grupo Proyección, Seguridad e Implementación.
3. Realizar la identificación de los riesgos y el registro de activos de información, su valoración en cuanto a las dimensiones de Confidencialidad, Integridad, Disponibilidad y el análisis de probabilidad e impacto de los riesgos. - Entrevistas-	Mayo-Septiembre de 2019	Oficial de Seguridad de la Información , Grupo Proyección, Seguridad e Implementación Tecnologíca con el apoyo del líder del proceso Gestión de Tecnología e Información, coordinadores de los Grupos Administración de la Información , Administración de las Tecnologías de la Información, Apoyo Seguridad Electrónica y propietarios de sistemas y activos de información.
4. Interpretar los resultados obtenidos del análisis del riesgo, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.	Octubre - Noviembre de 2019	
5. Seguimiento y control	Se realizara una reunión dos días después de cada fecha final de actividadades para presentar el informe del avance del proyecto y de esta manera evaluar los pasos que se han ido realizado.	Oficial de Seguridad de la Información, Coordinador Grupo Proyección, Seguridad e Implementación.

Tabla No 1. Cronograma de actividades.

4. Entregables

- Informe diagnóstico.
- Matriz de Valoración de Activos y Análisis de Riesgos de la Seguridad de la Información código PA-TI-M01-F01 diligenciada.
- Informe de los resultados obtenidos del análisis del riesgo.
- Actas de reuniones.

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, 09/07/2016.
- Norma Técnica NTC-ISO-IEC COLOMBIANA 27001. 2013/12/11. Sistemas de Gestión de la Seguridad de la Información.
- Norma Técnica NTC-ISO-IEC COLOMBIANA 27005. 2009/08/19. Gestión del Riesgo en Seguridad de la Información.

Anexos
• Anexo 1: PA-TI-M01 Metodología de Gestión y Evaluación de Riesgos de Seguridad de la Información
• Anexo 2: 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

Elaboró		Revisó		Aprobó	
Nombre:	María Cristina Reyes Castillo	**Nombre:**	Juan Manuel Riaño Vargas	**Nombre:**	Adriana Cetina Hernández
Cargo:	Auxiliar Administrativo	**Cargo:**	Jefe Oficina Asesora de Planeación	**Cargo:**	Jefe Oficina Sistemas de Información
Fecha:	28/Nov/2018	**Fecha:**	13/Dic/2018	**Fecha:**	13/Dic/2018
		Nombre:	Angélica María Patiño García		
		Cargo:	Profesional Especializado		
		Fecha:	13/Dic/2018		