



Oficina de Tecnología

Plan de Seguridad y Privacidad de la Información

Versión 1.0
Diciembre 23 de 2020



Tabla de contenido

Glosario	41.
Objetivos	42.
Alcance	53.
Política de Seguridad y Privacidad de la Información y Seguridad Digital de la USPEC	54.
Comité de Seguridad y Privacidad de la Información en la entidad	5.
Alcance del Plan de Seguridad y Privacidad de la Información	7
6. Formulación del Plan de Tratamiento de Riesgos de Seguridad y privacidad de la información	67.
Seguimiento	7

Introducción

A través del decreto 1008 del 14 de junio de 2018 se establecieron los lineamientos generales de la política de Gobierno Digital. En el mismo se establecen dos componentes o líneas de acción de esta política: TIC para el estado y TIC para la sociedad y establece tres habilitadores transversales que permitirán el cumplimiento de los logros establecidos en el decreto mencionado, estos habilitadores son Arquitectura de TI, Servicios ciudadanos digitales y Seguridad y privacidad.

Mediante el habilitador de seguridad y privacidad de información se busca que las entidades del estado implementen los lineamientos de seguridad de la información en todos sus activos de información, para el caso de la USPEC se incluyen datos, software, hardware, recurso humano y servicios, con el fin de preservar la confidencialidad, integridad y disponibilidad y privacidad de los datos.



En tal sentido se hace necesario continuar con la implementación y apropiación de lineamientos y controles en materia de seguridad de información que permitan fortalecer los tres pilares de la seguridad de información como lo son la confidencialidad, integridad y disponibilidad de la información institucional, para ello surge la necesidad de actualizar el plan de seguridad y privacidad de información, generando seguimientos trimestrales que permitan verificar el cumplimiento de las actividades propuestas.

Glosario

- **Confidencialidad:** propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
- **Disponibilidad:** propiedad de la información de estar accesible y utilizable cuando lo requiera un usuario autorizado.
- **Integridad:** propiedad de la información relativa a su exactitud y completitud
- **MSPI.** Modelo de seguridad y privacidad de información
- **SGSI.** Sistema de gestión de seguridad de la información

1. Objetivos

1.1 Objetivo General

Establecer las actividades requeridas para el fortalecimiento del MSPI a través de la actualización del plan de seguridad y privacidad de la información, con el fin propender por el mejoramiento continuo del SGSI.

1.2 Objetivos Específicos

- Fortalecer la infraestructura tecnológica de la Entidad a través de la identificación de vulnerabilidades y la implementación de planes de remediación.
- Actualizar los planes de tratamiento para la mitigación de riesgos de seguridad digital.
- Sensibilizar al personal de la Entidad en la aplicación de las políticas y lineamientos establecidos por el SGSI para la protección de la información institucional.
- Implementar acciones encaminadas a evidenciar la mejora continua del Sistema de Gestión de Seguridad y Privacidad de Información de la Entidad.

2. Alcance

El plan de seguridad y privacidad de la información involucra la norma NTC/ISO 27001:2013, los lineamientos establecidos a través del Modelo de Seguridad y Privacidad de Información – MSPI definido por el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, las políticas y procedimientos internos del SGSI y aplica para todos los procesos incluidos en el mapa de procesos institucional de la USPEC, así como todo el personal que forma parte de la Entidad.

3. Política de Seguridad y Privacidad de la Información y Seguridad Digital de la USPEC

A través de la resolución 000683 del 17 de diciembre de 2020 se aprobó la actualización de la Política de Seguridad y Privacidad de Información a través de la cual se establece que:

“La UNIDAD DE SERVICIOS PENITENCIARIOS Y CARCELARIOS, a través de la implementación del Modelo de Seguridad y privacidad de Información – MSPI, enmarcado en el Sistema de Gestión de Seguridad de Información y consciente de la importancia que representa la seguridad de la información y considerándola como un factor fundamental para la gestión y operación del suministro de bienes y prestación de servicios, la infraestructura y el apoyo logístico y administrativo requeridos para el adecuado funcionamiento de los servicios penitenciarios y carcelarios a cargo del INPEC, se compromete a preservar la confidencialidad, integridad y disponibilidad de la información a través de la gestión de los riesgos, cumplimiento de los objetivos de seguridad de la información, de los requisitos legales y organizacionales, de las obligaciones contractuales, y de la asignación de los recursos necesarios para mejorar continuamente el Sistema de Gestión de Seguridad de la Información”.

Adicionalmente se establecen los objetivos de seguridad de información, los roles y responsabilidades de todo el personal de la Entidad para el cumplimiento de la política, las políticas adicionales de seguridad de información y las directrices en caso de incumplimiento de la política.

4. Alcance del Plan de Seguridad y Privacidad de la Información

El presente plan de seguridad de información aplica para los procesos incluidos en el mapa de procesos institucional de la USPEC, así como todo el personal que forma parte del mismo.

5. Formulación del Plan de Seguridad y privacidad de la información

Este plan cuenta con una serie de actividades enmarcadas dentro del ciclo PHVA (Planear, Hacer, Verificar y Actuar) que se desarrollarán en el transcurso del 2021. Cabe mencionar que para el desarrollo de estas actividades se requiere contar principalmente con el apoyo de los líderes de cada proceso institucional y cada uno de sus delegados.

Iniciativa	Actividad	Responsable	Fecha inicio	Fecha fin	Porcentaje Programado por Trimestre			
					I	II	III	IV
Pruebas de vulnerabilidad y ethical hacking	Gestionar la contratación de las pruebas de vulnerabilidad y ethical hacking	Oficina de Tecnología	1/4/2021	31/10/2021	0%	50%	50%	0%
	Definir y ejecutar plan de pruebas de vulnerabilidad y ethical hacking	Contratista - Oficina de Tecnología	1/7/2021	30/12/2021	0%	0%	50%	50%
	Ejecutar plan de remediación de vulnerabilidades vigencia 2020	Oficina de Tecnología	4/1/2021	31/7/2021	50%	50%	0%	0%
Plan de tratamiento de riesgos de seguridad de información	Realizar seguimiento al plan de tratamiento de riesgos de seguridad de información	Oficina de Tecnología	23/3/2021	31/12/2021	25%	25%	25%	25%
Plan de comunicación, sensibilización y capacitación en seguridad de información	Ejecutar plan de comunicación, sensibilización y capacitación en seguridad de información	Oficina de Tecnología - Grupo Talento Humano - Prensa	8/2/2021	30/12/2021	25%	25%	25%	25%

Auditoria Externa al SGSI	Gestionar la contratación de la auditoria externa al SGSI	Oficina de Tecnología	11/5/2021	31/10/2021	0%	50%	50%	0%
	Ejecutar la auditoria externa al SGSI	Contratista - Oficina de Tecnología	1/9/2021	30/11/2021	0%	0%	10%	90%
	Elaborar plan de mejoramiento producto de la auditoria externa - 2020	Dependencias involucradas	1/12/2021	23/12/2021	0%	0%	0%	100%
Plan de Mejoramiento	Realizar seguimiento al plan de mejoramiento	Oficina de Tecnología	1/7/2021	31/12/2021	0%	0%	50%	50%
Estado del SGSI (Revisión por la Dirección)	Evaluar el estado general del SGSI	Oficina de Tecnología	1/7/2021	30/12/2021	0%	0%	50%	50%
Gestión de indicadores de seguridad de información	Realizar seguimiento a los indicadores del SGSI	Oficina de Tecnología	1/2/2021	30/12/2021	25%	25%	25%	25%
Plan de continuidad TI	Ejecutar pruebas del plan de continuidad de TI	Oficina de Tecnología	1/5/2021	30/11/2021	0%	50%	0%	50%

6. Seguimiento

El seguimiento al plan de seguridad y privacidad de información se realizará cada trimestre de acuerdo a la matriz establecida para tal fin recopilando tanto evidencias como descripción de acciones ejecutadas.

Aprobó:
 Andres Ernesto Díaz Hernández
 Jefe Oficina de Tecnología (E)

Revisó:
 Camilo Alejandro Romero González
 Coordinador Grupo Comunicaciones - Oficina de Tecnología

Elaboró:
 Mayra Alexandra Agudelo Carvajal
 Profesional Especializado

