



USPEC
UNIDAD DE SERVICIOS
PENITENCIARIOS Y CARCELARIOS

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
OFICINA DE TECNOLOGÍA

Oficina de Tecnología
Plan de Seguridad y Privacidad de la

Versión 1.0
Enero 31 de 2020



Tabla de contenido

Introducción.....	3
Glosario.....	3
1. Objetivos.....	4
1.1 Objetivo General.....	4
1.2 Objetivos Especificos	4
2. Alcance	4
3. Política de Seguridad y Privacidad de la Información y Seguridad Digital de la USPEC	4
4. Comité de Seguridad y Privacidad de la Información en la entidad	4
5. Alcance del Plan de Seguridad y Privacidad de la Información	5
6. Formulación del Plan de Tratamiento de Riesgos de Seguridad y privacidad de la información	5
7. 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.

En el año 2015 la entidad inició la implementación del Sistema de Gestión de Seguridad de Información en sus procesos institucionales. Como parte de los logros alcanzados se han definido inventario de activos, riesgos de seguridad digital, planes de tratamiento para mitigar los riesgos. Así mismo se ha buscado fortalecer otros aspectos relevantes como lo son la sensibilización y formación del personal que labora en la entidad y el fortalecimiento de la seguridad informática a través de nuevas herramientas que han permitido robustecer la infraestructura tecnológica que soporta la operación de los procesos institucionales.

En tal sentido se hace necesario continuar con la implementación y apropiación de lineamientos 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, así como la gestión y operación de la Entidad asociada con el suministro de bienes y la prestación de los servicios, la infraestructura física y el apoyo logístico y administrativo requeridos para el adecuado funcionamiento de los servicios penitenciarios y carcelarios a cargo del Instituto Nacional Penitenciario y Carcelario - INPEC, los cuales tienen como beneficiarios a las Personas Privadas de la Libertad.

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
- **SGSI.** Sistema de gestión de seguridad de la información

1. Objetivos

1.1 Objetivo General

Establecer las actividades requeridas para el fortalecimiento del Modelo de Seguridad y Privacidad de Información a través de la estructuración del plan de seguridad y privacidad de la información con el fin mitigar riesgos de seguridad digital asociados a pérdida de confidencialidad, integridad y disponibilidad de los activos de información de la USPEC,

1.2 Objetivos Específicos

- Fortalecer la infraestructura tecnológica de la Entidad a través de la identificación de vulnerabilidades y la implementación de planes de mitigación.
- Actualizar los planes de tratamiento para la mitigación de riesgos de seguridad digital.
- Sensibilizar al personal de la Entidad y partes interesadas 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 000705 del 10 de octubre de 2019 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.

4. Comité de Seguridad y Privacidad de la Información en la entidad

Actualmente la gestión requerida en este comité la asume el Comité Institucional de Gestión y Desempeño, creado a través de la Resolución 152 de 28 de febrero de 2018. Así mismo a través de la

resolución 000705 del 2019 se establecen como responsabilidades para el Sistema de Gestión de Seguridad de Información las siguientes:

- Coordinar la implementación del Modelo de Seguridad y privacidad de la Información al interior de la Entidad.
- Revisar los diagnósticos del estado de la seguridad de la información
- Acompañar e impulsar el desarrollo de proyectos de seguridad.
- Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos.
- Realizar revisiones periódicas del SGSI (por lo menos cada 12 meses) y según los resultados de esta revisión definir las acciones pertinentes.
- Promover la difusión y sensibilización de la seguridad de la información dentro de la Entidad.
- Las demás funciones inherentes a la naturaleza del Comité.

5. 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.

6. Formulación del Plan de Tratamiento de Riesgos 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 2020. 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.

No.	Iniciativa	Fase	Actividad	Producto	Recursos estimados	Responsable	Indicador	Fecha inicio	Fecha fin	Trim. I	Trim. II	Trim. III	Trim. IV
										P	P	P	P
1	Pruebas de vulnerabilidad y ethical hacking	Planear	Definir los estudios previos para la contratación de las pruebas de vulnerabilidad y ethical hacking	Estudio previo	\$102.000.000	Oficina de Tecnología	Binario	02-01-2020	15-02-2020	100%	0%	0%	0%
		Planear	Publicar en el portal del SECOP el proceso para la contratación de las pruebas de vulnerabilidad y ethical hacking	Estudio previo publicado en el SECOP		Dirección de Gestión Contractual	Binario	16-02-2020	13-03-2020	100%	0%	0%	0%
		Planear	Gestionar la perfección del contrato	Contrato		Dirección de Gestión Contractual	Binario	16-03-2020	28-03-2020	100%	0%	0%	0%
		Planear	Definir plan de pruebas de vulnerabilidad y ethical hacking	Plan de pruebas de vulnerabilidad		Contratista - Oficina de Tecnología	Binario	01-04-2020	30-04-2020	0%	100%	0%	0%
		Hacer	Ejecutar plan de pruebas de vulnerabilidad y ethical hacking	Informe de ejecución del plan de pruebas		Contratista - Oficina de Tecnología	Número de pruebas ejecutadas / Número total de pruebas programadas	01-05-2020	31-12-2020	0%	30%	30%	40%

2	Plan de tratamiento de riesgos de seguridad de información	Planear	Actualizar plan de tratamiento de riesgos de seguridad de información	Plan de tratamiento de riesgos actualizado	\$0	Todas las dependencias	Binario	01-01-2020	31-03-2020	100 %	0%	0%	0%
		Planear	Aprobar plan de tratamiento de riesgos de seguridad de información	Acta de aprobación de plan de tratamiento de riesgos		Líderes de proceso	Binario	27-01-2020	31-03-2020	100 %	0%	0%	0%
		Verificar	Realizar seguimiento al plan de tratamiento de riesgos de seguridad de información	Informe de ejecución del plan de tratamiento de riesgos		Oficina de Tecnología	Binario	01-02-2020	31-12-2020	25%	25%	25%	25%
3	Plan de comunicación, sensibilización y capacitación en seguridad de información	Planear	Definir propuesta plan de comunicación, sensibilización y capacitación en seguridad de información	Borrador del plan	\$0	Oficina de Tecnología	Binario	01-02-2020	10-03-2020	50%	50%	0%	0%
		Planear	Aprobar plan de comunicación, sensibilización y capacitación en seguridad de información	Plan aprobado		Grupo Talento Humano	Binario	10-03-2020	31-03-2020	100 %	0%	0%	0%
		Hacer	Ejecutar plan de comunicación, sensibilización y capacitación en seguridad de información	Informe de ejecución del plan		Oficina de Tecnología - Grupo Talento Humano - Prensa	Número de actividades ejecutadas / Número total de actividades programadas	01-04-2020	31-12-2020	0%	25%	25%	50%
4	Auditoria Externa al SGSI	Planear	Gestionar la contratación de la auditoria externa al SGSI	Estudio previo	\$15.000.000	Oficina de Tecnología	Binario	01-05-2020	30-05-2020	0%	0%	100 %	0%
		Planear	Publicar en el portal del SECOP el proceso para la contratación de la auditoria externa	Estudio previo publicado en el SECOP		Dirección de Gestión Contractual	Binario	01-06-2020	30-06-2020	0%	0%	100 %	0%
		Planear	Gestionar la perfección del contrato	Contrato		Dirección de Gestión Contractual	Binario	01-07-2020	31-07-2020	0%	0%	100 %	0%
		Verificar	Ejecutar la auditoria externa al SGSI	Productos establecidos en el procedimiento de Auditoria interna de la Entidad		Contratista - Oficina de Tecnología	Binario	01-10-2020	31-10-2020	0%	0%	0%	100 %
		Actuar	Elaborar plan de mejoramiento producto de la auditoria externa - 2020	Plan de mejoramiento		Dependencias involucradas	Binario	01-11-2020	30-11-2020	0%	0%	0%	100 %

5	Documentación del SGSI	Hacer	Actualizar documentación del SGSI	Documentación actualizada	\$0	Oficina de Tecnología - Dependencias involucradas	Binario	01-02-2020	30-06-2020	50%	50%	0%	0%
		Hacer	Actualizar indicadores del SGSI	Indicadores actualizados		Oficina de Tecnología	Binario	01-02-2020	30-06-2020	50%	50%	0%	0%
6	Plan de mejoramiento 2019	Verificar	Realizar seguimiento al plan de mejoramiento	Acciones con seguimiento	\$0	Oficina de Tecnología	Binario	01-02-2020	31-12-2020	0%	50%	0%	50%
7	Estado del SGSI (Revisión por la Dirección)	Verificar	Evaluar el estado general del SGSI	Informe de revisión por la Dirección	\$0	Oficina de Tecnología	Binario	01-02-2020	30-09-2020	50%	0%	50%	0%

7. Seguimiento

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

Revisó: Oscar Javier Suárez Ramos
Jefe Oficina de Tecnología

Elaboró: Mayra Alexandra Agudelo Carvajal
Profesional Especializado