USPEC
UNIDAD DE SERVICIOS
PENITENCIARIOS Y CARCELARIOS

PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

UNIDAD DE SERVICIOS PENITENCIARIOS Y CARCELARIOS

2023

USPEC
UNIDAD DE SERVICIOS
PENITENCIARIOS Y CARCELARIOS

Control de Versiones

Versión	Fecha	Modificación
1.0	17/01/2022	Se crea el plan estratégico de seguridad de información.
2.0	23/01/2023	Se actualiza el plan estratégico de seguridad de información

1. OBJETIVO

Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de la Unidad de Servicios Penitenciarios y Carcelarios - USPEC, con el fin de reducir a niveles aceptables los riesgos a los que está expuesta la entidad, a partir de la implementación de la estrategia de seguridad digital definida en este documento para la vigencia 2023.

1.1 OBJETIVOS ESPECÍFICOS

- ✓ Actualizar la estrategia de seguridad digital de la USPEC.
- ✓ Establecer las necesidades de la USPEC para la implementación del Sistema de Gestión de Seguridad de la Información.
- ✓ Priorizar los proyectos a implementar para la correcta implementación del SGSI.

2. ALCANCE

El Plan Estratégico de Seguridad de la Información al buscar el mantenimiento del Sistema de Gestión de Seguridad de la Información y la implementación de la estrategia de seguridad digital de la USPEC, comparte el alcance definido dentro de la Política de Seguridad, Privacidad de la Información y Seguridad Digital de la Entidad, a través de la cual se indica que el alcance del SGSI aplica a todos los procesos institucionales.

3. DOCUMENTOS DE REFERENCIA

El Plan Estratégico de Seguridad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

- ✓ Decreto 767 de 2022. "*Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"*
- ✓ Decreto 612 de 2018, "*Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado*", donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.
- ✓ Resolución 500 de 2021. "*Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital*".
- ✓ Manual de Gobierno Digital. Este documento establece los lineamientos y estándares de los componentes de la política (TIC para el Estado y TIC para la Sociedad) y de los habilitadores transversales (arquitectura, seguridad y privacidad de la información y servicios ciudadanos digitales).
- ✓ Modelo de Seguridad y Privacidad de la Información. (Actualizado a través de la Resolución 500 de 2021, definido por el Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC)
- ✓ Política de Seguridad, Privacidad de Información y Seguridad Digital de la USPEC (Actualmente creada bajo resolución 000181 de 2022)

4. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Actualmente la USPEC cuenta con un Sistema de Gestión de Seguridad de Información, establecido a través de la Política de seguridad, privacidad de información y seguridad digital (Resolución 000181 DE 2022). En ella se definen los objetivos de seguridad, los roles y las responsabilidades y las políticas específicas de seguridad de información, adicionalmente se cuenta con un conjunto de procedimientos que definen las actividades y controles que se requieren ejecutar por parte del personal de la USPEC para proteger la información institucional. Así como otros lineamientos establecidos a través de manuales, instructivos y guías de seguridad de información. Cabe mencionar que la documentación propia del SGSI se ha establecido con base en los controles definidos en la Norma ISO 27001 y se continuará con su actualización de acuerdo a su última versión vigente.

Para llevar a cabo la implementación de controles de seguridad de información se cuenta con un Manual de clasificación de activos que permite en primera instancia definir o actualizar los inventarios de activos por cada proceso, labor que se llevó a cabo durante el 2022. Así mismo se cuenta con una política de administración de riesgos, bajo la cual se actualizan los riesgos de seguridad de información y para su mitigación se establece con cada dependencia involucrada el respectivo plan de tratamiento de riesgos. Trimestralmente la Oficina de Tecnología se encarga de realizar seguimiento a la implementación del este plan, con el fin de verificar su estado de cumplimiento. Durante la vigencia anterior se llevó a cabo adicionalmente la actualización del mapa de riesgos de seguridad de información y su respectivo plan de tratamiento, dicho plan se implementará durante el 2023.

Con el fin de fortalecer la toma de conciencia frente a los lineamientos del SGSI, se cuenta con un plan de comunicación, sensibilización y capacitación en seguridad de información. Con el fin de evaluar su implementación se lleva a cabo el seguimiento trimestral a las actividades ejecutadas.

Para llevar a cabo la medición del SGSI se realiza periódicamente el seguimiento a los indicadores de seguridad de información, estos se enfocan en la evaluación de la ejecución del plan de tratamiento de riesgos de seguridad de información, la gestión de incidentes y la gestión de vulnerabilidades de la plataforma tecnológica.

Para evaluar el estado de implementación del SGSI, se llevan a cabo ejercicios de auditoria interna y producto de los mismos se elaboran los planes de mejoramiento. La Oficina de Control Interno se encarga de realizar seguimiento de forma periódica con el fin de determinar el cumplimiento de las acciones propuestas. La última auditoria se inició a finales del 2022, incluyendo como alcance el Modelo de Seguridad y Privacidad de Información - MSPI, establecido por MINTIC y la Norma ISO 27001:2013.

5. ESTRATEGIA DE SEGURIDAD DIGITAL

LA USPEC actualiza su estrategia de seguridad digital en la que se integren las políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira entorno a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, así como la política de administración de riesgos de la entidad y el procedimiento de gestión de eventos e incidentes de seguridad de información, tal como se establece en la Resolución 500 de 2021.

Por tal motivo, la USPEC define las siguientes 6 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:

5.1 DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar:

ESTRATEGIA	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad de la información	Asegurar que se mantenga el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la actualización de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de procesos institucionales, a través del establecimiento de los roles y responsabilidades en seguridad de la información.
Gestión de riesgos de seguridad de información	Evaluar la gestión realizada en el 2021 frente a los riesgos de seguridad de la información, con el fin de llevar a cabo su actualización de acuerdo a la metodología establecida por la Entidad, buscando prevenir o reducir los efectos indeseados a través de la implementación de controles de seguridad.
Implementación del plan de tratamiento de riesgos de seguridad de información	Planear, implementar y realizar seguimiento a las acciones requeridas para mitigar los riesgos que pueden afectar la seguridad física y digital, tomando como referencia los controles establecidos en la Norma ISO 27001.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.
Concientización, sensibilización y capacitación	Fortalecer la cultura organizacional tomando como referencia los lineamientos establecidos en la Entidad a través del sistema de gestión de seguridad de la información, con el fin de promover una conciencia entre el personal para la protección de la información institucional.
Medición, revisión y evaluación del SGSI	Evaluar el sistema de gestión de seguridad de información periódicamente, con el fin de determinar el cumplimiento de las actividades y metas establecidas y generar acciones en pro de la mejora continua.
Relación con proveedores de seguridad digital	Al llevar a cabo la adquisición de productos y servicios para la gestión de la seguridad digital de la entidad, se pueden otorgar permisos a los proveedores que les permitan acceder a la información institucional, como a los sistemas de información o así mismo proporcionar activos de software, hardware y/o recursos humanos que estén involucrados en el procesamiento de información. En tal sentido es de vital importancia establecer los controles que permitan mitigar posibles riesgos de seguridad digital que se puedan generar en la gestión con los proveedores.

5.2 PORTAFOLIO DE PROYECTOS:

Para cada estrategia específica, la USPEC define los siguientes proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI):

EJE	PROYECTO	PRODUCTOS ESPERADOS
Liderazgo de seguridad de la información	**Proyecto1:** Implementar los procedimientos, políticas y demás lineamientos del SGSI.	1. Política de Seguridad y privacidad de información actualizada, publicada, aprobada y socializada.
Gestión de riesgos	**Proyecto 2**: Actualizar los riesgos de seguridad de información.	1. Matriz de riesgos de seguridad digital actualizada.
		2. Aprobación de la actualización de los riesgos de seguridad de información
Concientización, sensibilización y capacitación	**Proyecto 3:** Gestionar el plan de sensibilización, capacitación y comunicación en seguridad de información.	1. Plan de Sensibilización, comunicación y capacitación actualizado.
		2. Evidencias de las actividades ejecutadas
		3. Seguimiento de actividades
		4. Resultado de las encuestas de medición
Implementación del plan de tratamiento de riesgos de seguridad de información	**Proyecto 4:** Gestionar el plan de tratamiento de riesgos de seguridad de información.	1. Informe trimestral de seguimiento al plan de tratamiento de riesgos de seguridad de información.
Gestión de incidentes	**Proyecto 5:** Llevar a cabo la gestión de incidentes conforme a lo establecido en el Procedimiento de gestión de eventos e incidentes de seguridad de información	1. Análisis de indicador de gestión de incidentes
		2. Soportes de análisis de eventos y/o incidentes

Medición, revisión y evaluación del SGSI	**Proyecto 6:** Gestionar los indicadores de seguridad de información	1. Indicadores actualizados
		2. Reporte de seguimiento a indicadores
	Proyecto 7: Revisar el avance del Sistema de gestión de seguridad de información.	1. Informe semestral de revisión por la dirección.
	Proyecto 8: Auditoria externa de seguridad de información	1. Plan de auditoria
		2. Listas de verificación
		3. Informe de auditoria
	Proyecto 9: Gestionar el plan de mejoramiento de seguridad de información.	1. Plan de mejoramiento actualizado
		2. Seguimiento al plan de mejoramiento
Relación con proveedores de seguridad digital	**Proyecto 10:** Implementar lineamientos para la gestión con los proveedores de TI.	1. Lineamientos para la gestión de proveedores de TI.

5.3 CRONOGRAMA DE ACTIVIDADES / PROYECTOS:

A continuación se presenta el cronograma de actividades a través del cual se evidencia como se llevarán a cabo cada uno de los proyectos relacionados en el punto anterior:

PROYECTO	ACTIVIDADES	PRODUCTOS ESPERADOS	RESPONSABLE	AÑO 2023			
				TRIM 1	TRIM 2	TRIM 3	TRIM 4
Eje: Liderazgo de seguridad de la información							
Proyecto1: Implementar los procedimientos, políticas y demás lineamientos del SGSI.	Aprobar, publicar y socializar la política de seguridad de información	1. Política de Seguridad y privacidad de información publicada, aprobada y socializada.	Dirección General - Responsable SGSI				X
Eje: Gestión de riesgos							
Proyecto 2: Actualizar los riesgos de seguridad de información.	Realizar mesas de trabajo con los responsables para llevar a cabo la actualización de las matrices de riesgos de seguridad de información por cada proceso institucional.	1. Matriz de riesgos de seguridad digital actualizada.	Responsable SGSI(Apoya la gestión) Todas las Dependencias				X
	Aprobar la matriz de riesgos de seguridad de información	2. Aprobación de la actualización de los riesgos de seguridad de información	Director o Jefe de cada dependencia - Comité Institucional de Gestión y Desempeño				X
Eje: Concientización, sensibilización y capacitación							
Proyecto 3: Gestionar el	Actualizar el plan de sensibilización, capacitación y comunicación en seguridad de información	1. Plan de Sensibilización, comunicación y capacitación actualizado.	Responsable SGSI	X			

plan de sensibilización, capacitación y comunicación en seguridad de información.	Realizar seguimiento trimestral al plan de comunicación, sensibilización y capacitación en seguridad de información.	2. Evidencias de las actividades ejecutadas	Responsable SGSI	X	X	X	X
		3. Seguimiento de actividades	Responsable SGSI	X	X	X	X
	Realizar encuestas para medir el grado de sensibilización del personal de la Entidad.	4. Resultado de las encuestas de medición	Responsable SGSI		X		X
Eje: Implementación del plan de tratamiento de riesgos de seguridad de información							
Proyecto 4: Gestionar el plan de tratamiento de riesgos de seguridad de información.	Realizar seguimiento trimestral al plan de tratamiento de riesgos de seguridad de información	1. Informe trimestral de seguimiento al plan de tratamiento de riesgos de seguridad de información.	Todas las dependencias (Reportar seguimiento) Responsable SGSI (Consolidar informe, realizar observaciones)	X	X	X	X
Eje: Gestión de incidentes							
Proyecto 5: Llevar a cabo la gestión de incidentes conforme a lo establecido en el Procedimiento de gestión de eventos e incidentes de seguridad de información	Realizar el análisis de los eventos y/o incidentes de seguridad de información, de acuerdo al reporte realizado por los usuarios.	1. Análisis de indicador de gestión de incidentes	Responsable SGSI - Equipo de gestión de incidentes				X
		2. Soportes de análisis de eventos y/o incidentes					
Eje: Medición, revisión y evaluación del SGSI							

Proyecto 6: Gestionar los indicadores de seguridad de información	Actualizar los indicadores de seguridad de información	1. Indicadores actualizados	Responsable SGSI	X			
	Realizar seguimiento periódico a los indicadores de seguridad de información	2. Reporte de seguimiento a indicadores	Responsable SGSI	X	X	X	X
Proyecto 7: Revisar el avance del Sistema de gestión de seguridad de información.	Realizar el informe semestral de revisión por la dirección.	1. Informe semestral de revisión por la dirección.	Responsable SGSI		X		X
Proyecto 8: Auditoria externa de seguridad de información	Definir el plan de auditoria y las listas de verificación	1. Plan de auditoria	Contratista			X	X
		2. Listas de verificación	Contratista			X	X
	Ejecutar el plan de auditoria	3. Informe de auditoria	Contratista			X	X
Proyecto 9: Gestionar el plan de mejoramiento de seguridad de información.	Actualizar el plan de mejoramiento de seguridad de información	1. Plan de mejoramiento actualizado	Dependencias involucradas - Responsable SGSI (Apoya la gestión)				X
	Realizar seguimiento al plan de mejoramiento de seguridad de información	2. Seguimiento al plan de mejoramiento	Responsable SGSI		X		X
Proyecto 10: Implementar lineamientos para la gestión con los proveedores de TI.	Definir los lineamientos para llevar a cabo la gestión de los proveedores de TI, de acuerdo a lo establecido a través de la Resolución 500 de 2021	1.Lineamientos para la gestión de proveedores de TI	Oficina de Tecnología				X

5.4 ANÁLISIS PRESUPUESTAL:

A continuación, se presenta el presupuesto referente al Sistema de Gestión de Seguridad de Información, establecido y aprobado a través del plan anual de adquisiciones:

AÑO 2023	
PROYECTO	**PRESUPUESTO**
Solución tecnológica integral: ✓ Backup ✓ Antivirus ✓ Herramientas seguridad informática ✓ Ethical hacking ✓ Auditoria al SGSI ✓ Certificados digitales	$ 685.000.000

6. APROBACIÓN

El presente plan ha sido sometido a consideración y conocimiento de la alta dirección, el comité de gestión y desempeño institucional con el objetivo de ser aprobado y aplicado conforme a lo que aquí se define.

ELABORÓ	REVISÓ	APROBÓ
Nombre: Mayra Alexandra Agudelo Carvajal Cargo: Profesional Especializado Dependencia: Oficina de Tecnología	Nombre: Imelda Muñoz Mancipe Cargo: Jefe Oficina de Tecnología Dependencia: Oficina de Tecnología	Comité Institucional de Gestión y Desempeño