USPEC
UNIDAD DE SERVICIOS
PENITENCIARIOS Y CARCELARIOS

PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

UNIDAD DE SERVICIOS PENITENCIARIOS Y CARCELARIOS

2022

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.

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 2022.

1.1 OBJETIVOS ESPECÍFICOS

- ✓ Definir y establecer la estrategia de seguridad digital de la USPEC.
- ✓ Definir y 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.
- ✓ Planificar la evaluación y seguimiento de los controles y lineamientos implementados en el marco del Sistema de Gestión de Seguridad de la Información.

2. ALCANCE

El Plan Estratégico de Seguridad de la Información al buscar la implementación del Sistema de Gestión de Seguridad de la Información y la estrategia de seguridad digital de la USPEC, comparte el alcance definido dentro de la Política de Seguridad y Privacidad de la Información de la Entidad, a través de la cual se 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 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 – MINTIC.
- ✓ Modelo de Seguridad y Privacidad de la Información – MINTIC.
- ✓ Política de Seguridad y Privacidad de Información de la USPEC (Actualmente creada bajo resolución 000683 de 2020)

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 y privacidad de información (Resolución 000683 DE 2020). 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. Cabe mencionar que la documentación propia del SGSI se estableció con base en lo establecido en la Norma ISO 27001:2013.

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 encuentra pendiente por actualizar de acuerdo a los últimos lineamientos establecidos por la Entidad. 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 el 2021 se logró un avance de implementación del plan del 93.5%.

Con el fin de fortalecer la toma de conciencia frente a los lineamientos del SGSI, se cuenta con una 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 realizó en el mes de noviembre del 2021 y su alcance incluyó aquellos procesos que contaban con riesgos de seguridad de información y se realizó tomando como referencia el Modelo de Seguridad y Privacidad de Información - MSPI, establecido por MINTIC y la Norma ISO 27001:2013. Como producto de su ejecución se generaron xx no conformidades, con las cuales se elaboró el plan de mejoramiento para ejecutar en el 2022.

5. ESTRATEGIA DE SEGURIDAD DIGITAL

LA USPEC establecerá una 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 el Anexo A de la Norma ISO 27001:2013.
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 continúa.

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 publicada, aprobada y socializada.

Gestión de riesgos	**Proyecto 1**: Actualizar los inventarios de activos de información de los procesos institucionales, de acuerdo a la metodología establecida por la Entidad.	1. Inventarios de activos actualizados
		2. Aprobación de actualización de inventarios de activos
	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 1:** 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 1:** Gestionar el plan de tratamiento de riesgos de seguridad de información.	1. Plan de tratamiento de riesgos de seguridad actualizado.
		2. Plan de tratamiento de riesgos de seguridad aprobado y publicado
		3. Informe trimestral de seguimiento al plan de tratamiento de riesgos de seguridad de información.
	Proyecto 2: Actualizar la declaración de aplicabilidad.	4. Declaración de aplicabilidad actualizada.
Gestión de incidentes	**Proyecto 1:** Llevar a cabo la gestión de incidentes conforme a lo establecido en la Resolución 500 de 2021.	1. Procedimiento de gestión de eventos e incidentes de seguridad de información actualizado, publicado y socializado

Medición, revisión y evaluación del SGSI	**Proyecto 1:** Gestionar el autodiagnóstico del MSPI	1. Matriz de autodiagnóstico actualizada
		2. Acta de necesidades de ajuste
	Proyecto 2: Gestionar los indicadores de seguridad de información	3. Indicadores actualizados
		4. Reporte de seguimiento a indicadores
	Proyecto 3: Revisar el avance del Sistema de gestión de seguridad de información.	5. Informe semestral de revisión por la dirección.
		6. Acta de reunión
	Proyecto 4: Auditoria externa de seguridad de información	7. Plan de auditoria
		8. Listas de verificación
		9. Informe de auditoria
	Proyecto 5: Gestionar el plan de mejoramiento de seguridad de información.	7. Plan de mejoramiento actualizado
		8. Seguimiento al plan de mejoramiento

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 2022			
				TRIM 1	TRIM 2	TRIM 1	TRIM 1
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 1: Actualizar los inventarios de activos de información de los procesos institucionales, de acuerdo a la metodología establecida por la Entidad.	Realizar mesas de trabajo con los responsables para llevar a cabo la actualización de los inventarios de activos por cada dependencia.	1. Inventarios de activos actualizados	Responsable SGSI (Apoya la gestión) Todas las Dependencias	X	X		
	Aprobar los inventarios de activos actualizados	2. Aprobación de actualización de inventarios de activos	Director o Jefe de cada dependencia		X		

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 dependencia.	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 1: Gestionar el plan de sensibilización, capacitación y comunicación en seguridad de información.	Actualizar el plan de sensibilización, capacitación y comunicación en seguridad de información	1. Plan de Sensibilización, comunicación y capacitación actualizado.	Responsable SGSI	X			
	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 1: Gestionar el plan de tratamiento de riesgos de seguridad de información.	Actualizar el plan de tratamiento de riesgos de seguridad de información	1. Plan de tratamiento de riesgos de seguridad actualizado.	Responsable SGSI (Apoya la gestión) Todas las Dependencias	X			
	Aprobar el plan de tratamiento de riesgos de seguridad de información	2. Plan de tratamiento de riesgos de seguridad aprobado y publicado	Director o Jefe de cada dependencia - Comité Institucional de Gestión y Desempeño	X			
	Realizar seguimiento trimestral al plan de tratamiento de riesgos de seguridad de información	3. 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

Proyecto 2: Actualizar la declaración de aplicabilidad.	Actualizar la declaración de aplicabilidad de acuerdo a la gestión de riesgos de seguridad realizada en el 2021.	4. Declaración de aplicabilidad actualizada.	Responsable SGSI		X		
Eje: Gestión de incidentes							
Proyecto 1: Llevar a cabo la gestión de incidentes conforme a lo establecido en la Resolución 500 de 2021.	Actualizar el procedimiento de gestión de eventos e incidentes de seguridad de información	1. Procedimiento de gestión de eventos e incidentes de seguridad de información actualizado, publicado y socializado	Responsable SGSI - Equipo de gestión de incidentes	X	X		
Eje: Medición, revisión y evaluación del SGSI							
Proyecto 1: Gestionar el autodiagnóstico del MSPI	Actualizar el autodiagnóstico MSPI	1. Matriz de autodiagnóstico actualizada	Responsable SGSI	X	X		
	Evaluar la necesidad de ajustar los planes de seguridad de información de acuerdo a los resultados del autodiagnóstico	2. Acta de necesidades de ajuste	Responsable SGSI		X		

Proyecto 2: Gestionar los indicadores de seguridad de información	Actualizar los indicadores de seguridad de información	3. Indicadores actualizados	Responsable SGSI	X			
	Realizar seguimiento periódico a los indicadores de seguridad de información	4. Reporte de seguimiento a indicadores	Responsable SGSI	X	X	X	X
Proyecto 3: Revisar el avance del Sistema de gestión de seguridad de información.	Realizar el informe semestral de revisión por la dirección.	5. Informe semestral de revisión por la dirección.	Responsable SGSI		X		X
	Tomar decisiones relevantes para la mejora continúa del SGSI	6. Acta de reunión	Comité institucional de gestión y desempeño			X	X
Proyecto 4: Auditoria externa de seguridad de información	Definir el plan de auditoria y las listas de verificación	7. Plan de auditoria	Contratista			X	X
		8. Listas de verificación	Contratista			X	X
	Ejecutar el plan de auditoria	9. Informe de auditoria	Contratista			X	X
Proyecto 5: Gestionar el plan de mejoramiento de seguridad de información.	Actualizar el plan de mejoramiento de seguridad de información	7. Plan de mejoramiento actualizado	Dependencias involucradas - Responsable SGSI (Apoya la gestión)				X
	Realizar seguimiento al plan de mejoramiento de seguridad de información	8. Seguimiento al plan de mejoramiento	Responsable SGSI		X		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 2022	
PROYECTO	**PRESUPUESTO**
Auditoria externa de seguridad de información	$ 35.000.000
Implementación de plan de tratamiento de riesgos seguridad de información – Ethical Hacking	$ 4.700.000.000 Nota: El proceso se encuentra incluido en la gestión de conectividad para los ERONES, se encuentra pendiente la desagregación de presupuesto para el proceso de contratación de ethical hacking.
Implementación de plan de tratamiento de riesgos seguridad de información - Antivirus	$60.000.000
Implementación de plan de tratamiento de riesgos seguridad de información - Solución tecnológica integral (herramientas de seguridad)	$ 570.000.000 Nota: La adquisición de herramientas de seguridad se encuentra incluido en el presupuesto de la solución tecnológica integral, se encuentra pendiente la desagregación de presupuesto.

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