UNIDAD DE SERVICIOS PENITENCIARIOS Y CARCELARIOS - USPEC

PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

VERSIÓN 3.0

USPEC
UNIDAD DE SERVICIOS
PENITENCIARIOS Y CARCELARIOS

TABLA DE CONTENIDO

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 2024.

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 actualización 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*".
- ✓ Resolución 1519 de 2020. "*Por la cual se definen los estándares y directrices para publicar la información señalada en la ley 1712 de 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos"*
- ✓ 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)
- ✓ Guía para la administración de riesgos y el diseño de controles de las entidades públicas, del Departamento Administrativo de la Función Pública - DAFP
- ✓ 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 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 de este plan, con el fin de verificar su estado de cumplimiento.

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 realizó a finales del 2023, 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 estratégicas específicas

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

ESTRATEGIA	DESCRIPCIÓN
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.

ESTRATEGIA	DESCRIPCIÓN
Gestión de riesgos de seguridad de información	Evaluar la gestión realizada en el 2023 frente a los riesgos de seguridad de la información, así como los resultados de la auditoría de seguridad de información realizada a finales de la misma vigencia, 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. Así mismo 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.
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.
Fortalecimiento de controles técnicos	En los últimos años los incidentes de seguridad de información han aumentado de manera considerable, generando robos de información, fraudes e incluso detener las operaciones de las organizaciones. En tal sentido es necesario reevaluar los controles que permiten blindar la plataforma tecnológica de la entidad y generar acciones que permitan su fortalecimiento ante posibles amenazas de cibserseguridad.
Transición de la Norma ISO 27001:2013 a la 27001:2022	La transición a ISO 27001:2022 responde a la necesidad de abordar las exigencias regulatorias actuales, ajustar la gestión de seguridad de la información a los escenarios tecnológicos actuales y sus amenazas y, de forma particular, optimizar el uso de los controles que conforman el Anexo A, agrupando algunos, suprimiendo otros e incorporando algunos nuevos. Estas modificaciones consideran temas de ciberseguridad, privacidad de datos y de información. [1] Por consiguiente es necesario para la Entidad, llevar a cabo este proceso de actualización, identificando aquellos cambios que se deben realizar al interior de la Entidad con el fin de fortalecer el SGSI.

6. Portafolio de actividades

Para cada estrategia específica, la USPEC define las actividades y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información. Estas actividades se encuentran definidas en la matriz del proyecto de implementación del Modelo de Seguridad y Privacidad de Información. (Ver documento anexo)

[1] https://www.escuelaeuropeaexcelencia.com/2023/06/transicion-a-iso-270012022-del-sistema-de-gestion-de-seguridad-de-la-informacion/#:~:text=La%20transici%C3%B3n%20a%20ISO%2027001%3A2022%20responde%20a%20la%20necesidad,el%20Anexo%20A%2C%20agrupando%20algunos%2C

7. 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:

PROYECTO	PRESUPUESTO
Solución tecnológica integral: ✓ Solución de ciberseguridad ✓ Herramientas seguridad informática ✓ Auditoria al SGSI ✓ Certificados digitales ✓ Ethical Hacking	$ 695.500.000

RESUMEN DE CAMBIOS

Versión	Fecha	Numerales	Descripción de la modificación
1.0	17/01/2022	Todos	Se crea el plan estratégico de seguridad de información.
2.0	23/01/2023	Todos	Se actualiza el plan estratégico de seguridad de información
3.0	15/01/2024	Todos	Se actualiza el plan estratégico de seguridad de información

RESPONSABILIDAD Y AUTORIDAD		
Elaboró / Actualizó:	**Revisó:**	**Aprobó:**
Firma: 	Firma: 	Firma: 
Nombre: Mayra Alexandra Agudelo Carvajal	Nombre: Imelda Muñoz Mancipe	Nombre: Imelda Muñoz Mancipe
Cargo: Profesional Especializado	Cargo: Jefe Oficina de Tecnología	Cargo: Jefe Oficina de Tecnología
Dependencia: Oficina de Tecnología	Dependencia: Oficina de Tecnología	Dependencia: Oficina de Tecnología
		Comité Institucional de Gestión y Desempeño Acta N. 25-01-24 del 25 de enero de 2024