USPEC
UNIDAD DE SERVICIOS
PENITENCIARIOS Y CARCELARIOS

Primer Trimestre de 2022
Presentado Abril 11 de 2022

Plan Estratégico de Seguridad y Privacidad de Información

Introducción

A través de la resolución 500 de 2021, *"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 en la cual se establece que los sujetos obligados deben adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital. Dicha estrategia se debe incluir en el Plan Estratégico de seguridad y privacidad de información que se integra al Plan de Acción en los términos artículo 2.2.22.3.14. del capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, o la norma que la modifique, adicione, subrogue o derogue.*

Así mismo 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 tal sentido la USPEC estableció una estrategia de seguridad digital para la gestión de la seguridad de la información, esta 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.

1. OBJETIVO

Realizar seguimiento a la implementación del Plan Estratégico de Seguridad y Privacidad de Información de la Unidad de Servicios Penitenciarios y Carcelarios - USPEC, con el fin de verificar la ejecución de las actividades propuestas para la vigencia 2022.

2. ESTRATEGIA DE SEGURIDAD DIGITAL

La USPEC definió su estrategia de seguridad digital a través de las siguientes 6 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:

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 de seguridad digital:

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

4. SEGUIMIENTO

ESTRATEGIA	PROYECTO	ACTIVIDAD	EJECUCIÓN
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	Se aprobó la Política de seguridad y privacidad de información por parte del Comité Institucional de Gestión y Desempeño el 11 y 12 de febrero de 2022. Se realizó el control de legalidad por parte de la Oficina Asesora Jurídica y se solicitó a la Dirección General la firma del documento. **Evidencias:** A. Borrador política de seguridad y privacidad de información B. Acta de Comité institucional de gestión y desempeño. C. Correo de control de legalidad. D. Correo de solicitud a la Dirección General.
Gestión de riesgos	Proyecto 1: Actualizar los inventarios de activos de información de los procesos	Realizar mesas de trabajo con los responsables para llevar a cabo la actualización de los inventarios de activos por cada dependencia.	La OTEC solicitó a través del memorando I2022-001130 de 8 de marzo 2022, la delegación de personal de cada uno de los procesos para llevar a cabo la actualización del inventario de activos de información, tarea que se está realizando en conjunto con el Grupo de Gestión Documental y la Oficina Asesora Jurídica.

ESTRATEGIA	PROYECTO	ACTIVIDAD	EJECUCIÓN
	institucionales, de acuerdo a la metodología establecida por la Entidad.		El 15 de marzo de 2022, se llevó a cabo la primera reunión de socialización del Manual de clasificación de activos con el personal delegado de cada dependencia. De un total de 18 funcionarios invitados a la reunión, asistieron 13 personas. Durante el primer trimestre se realizaron reuniones con los siguientes procesos para iniciar la actualización de información: ▪ Gestión Estratégica Organizacional ▪ Gestión de Infraestructura ▪ Gestión de Atención a Establecimientos de Reclusión ▪ Gestión Financiera ▪ Gestión de Atención al Ciudadano **Evidencias:** A. Memorando I2022-001130 de 8 de marzo 2022 B. Cronograma de actualización de inventarios C. 1 reunión actualización inventario de activos D. Resultados de reunion por dependencias.
		Aprobar los inventarios de activos actualizados	Una vez se culmine la actualización de información, se procederá con la actualización de los inventarios de activos por parte de cada líder de proceso y del Comité Institucional de Gestión y Desempeño.
	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.	De acuerdo al cronograma definido por la Oficina Asesora de Planeación y Desarrollo, esta actividad iniciará en el segundo trimestre del año.

ESTRATEGIA	PROYECTO	ACTIVIDAD	EJECUCIÓN
		Aprobar la matriz de riesgos de seguridad de información	Esta actividad depende de la actualización de los mapa de riesgos de seguridad de información.
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	Se llevó a cabo la actualización del plan de sensibilización, capacitación y comunicación en seguridad de información. **Evidencias**: A. Plan actualizado.
		Realizar seguimiento trimestral al plan de comunicación, sensibilización y capacitación en seguridad de información	Se ejecutaron las siguientes actividades: ▪ Se socializo a través de reunion virtual el manual de clasificación de activos con el personal delegado de cada proceso. ▪ Se elaboraron piezas con contenidos de tips seguros y se compartieron con todo el personal de la USPEC a través de correo institucional. ▪ Se elaboró por parte de la OTEC el cronograma de charlas de seguridad de información y se compartió a los Directivos y Jefes a través del memorando I2022-001153 de 9 de marzo de 2022. ▪ Se realizó la primera charla de seguridad de información, dirigida al personal de la Subdirección de Atención a Establecimientos de Reclusión. De un total de 86 personas citadas solo asistió el 30%. Posteriormente se remitió a los asistentes encuesta de evaluación con el tema tratado, de un total de 23 personas a las cuales se les compartió, solo participaron 12 de ellas. **Evidencias**: A. Evidencias socialización manual de clasificación de activos. B. Piezas tips seguros C. Cronograma charlas de seguridad de información

ESTRATEGIA	PROYECTO	ACTIVIDAD	EJECUCIÓN
			D. Memorando I2022-001153 de 9 de marzo de 2022 E. Evidencias primera charla seguridad de información – SUBAER
		Realizar encuestas para medir el grado de sensibilización del personal de la Entidad.	De acuerdo a la primera charla de seguridad de información que se realizó con el personal de la Subdirección de Atención a Establecimientos de Reclusión, se remitió encuesta de conocimientos sobre los temas tratados. El objetivo era realizar la encuesta al total de funcionarios de la SUBAER, sin embargo teniendo en cuenta que se pretendía evaluar la información brindada en la charla, solo se compartió con 26 los asistentes (26 funcionarios) y fue contestado solo por 12 de ellos, es decir que se obtuvo un porcentaje de participación del 46%. **Evidencias**: E. Encuesta charla de seguridad de información – correo.
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	Esta actividad depende de la actualización del mapa de riesgos de seguridad de información, de acuerdo a lo establecido por la OAPLA, la actividad iniciará en el segundo trimestre del 2022.
		Aprobar el plan de tratamiento de riesgos de seguridad de información	Esta actividad depende de la actualización del mapa de riesgos de seguridad de información, de acuerdo a lo establecido por la OAPLA, la actividad iniciará en el segundo trimestre del 2022.
		Realizar seguimiento trimestral al plan de tratamiento de riesgos de seguridad de información	Se realizó seguimiento al plan de tratamiento de riesgos de seguridad de información. En conclusión, de acuerdo a la información reportada por cada una de las dependencias, se obtuvo un porcentaje de avance del 19%.

ESTRATEGIA	PROYECTO	ACTIVIDAD	EJECUCIÓN
			Cabe mencionar que este plan se generó como producto de aquellas actividades definidas en el plan de tratamiento de riesgos 2021 y que al finalizar dicha vigencia, no se cumplieron en su totalidad. Se encuentra pendiente llevar a cabo la gestión de actualización del nuevo mapa de riesgos, de acuerdo a lo establecido por la OAPLA esta actividad iniciará en el segundo trimestre del año.
	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.	De acuerdo a lo programado en el plan estratégico de seguridad y privacidad de información, esta actividad iniciará en el segundo trimestre del 2022.
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	Durante el primer trimestre no fue posible iniciar la actualización del procedimiento de gestión de incidentes, teniendo en cuenta el alto volumen de trabajo del funcionario a cargo de la actividad. Se tiene previsto iniciar en el segundo trimestre.
Medición, revisión y evaluación del SGSI	Proyecto 1: Gestionar el autodiagnóstico del MSPI	Actualizar el autodiagnóstico MSPI	Se inició la actualización del autodiagnóstico del Modelo de seguridad y privacidad de información, este proceso incluye las secciones: ▪ Levantamiento de información ▪ Areas involucradas ▪ Administrativas ▪ Técnicas. Se encuentra en proceso de actualización ▪ PHVA. **Evidencias:** A. Autodiagnóstico MSPI

ESTRATEGIA	PROYECTO	ACTIVIDAD	EJECUCIÓN
		Evaluar la necesidad de ajustar los planes de seguridad de información de acuerdo a los resultados del autodiagnóstico	De acuerdo a lo programado en el plan estratégico de seguridad y privacidad de información, esta actividad iniciará en el segundo trimestre del 2022.
	Proyecto 2: Gestionar los indicadores de seguridad de información	Actualizar los indicadores de seguridad de información	Se llevó a cabo la actualización de los indicadores de seguridad de información, incluyendo la medición de la participación del personal de la USPEC en actividades de sensibilización del SGSI. En total se cuenta con 4 indicadores que permiten medir el desempeño del Sistema de gestión de seguridad de información, entre los cuales se encuentran: ▪ Gestión de indicadores ▪ Implementación del plan de tratamiento de riesgos de seguridad de información ▪ Gestión de vulnerabilidades ▪ Porcentaje de parcipación en actividades de seguridad de información
		Realizar seguimiento periódico a los indicadores de seguridad de información	De acuerdo a los tiempos establecidos para el reporte de incidentes se realizó el seguimiento al indicador Implementación del plan de tratamiento de riesgos, arrojando un resultado de 19% de avance de las actividades propuestas, con participación de los procesos: Talento Humano, Gestión Jurídica, Gestión de atención a establecimientos de reclusión, Gestión de tecnologías de la información.
	Proyecto 3: Revisar el avance del Sistema de gestión de seguridad de	Realizar el informe semestral de revisión por la dirección.	De acuerdo a lo programado en el plan estratégico de seguridad y privacidad de información, esta actividad iniciará en el segundo trimestre del 2022.

ESTRATEGIA	PROYECTO	ACTIVIDAD	EJECUCIÓN
	información.	Tomar decisiones relevantes para la mejora continúa del SGSI	De acuerdo a lo programado en el plan estratégico de seguridad y privacidad de información, esta actividad iniciará en el tercer trimestre del 2022.
	Proyecto 4: Auditoria externa de seguridad de información	Definir el plan de auditoria y las listas de verificación	De acuerdo a lo programado en el plan estratégico de seguridad y privacidad de información, esta actividad iniciará en el tercer trimestre del 2022.
		Ejecutar el plan de auditoria	De acuerdo a lo programado en el plan estratégico de seguridad y privacidad de información, esta actividad iniciará en el tercer trimestre del 2022.
	Proyecto 5: Gestionar el plan de mejoramiento de seguridad de información.	Actualizar el plan de mejoramiento de seguridad de información	Se actualizó el plan de mejoramiento de seguridad de información, el cual contiene las actividades requeridas para subsanar las no conformidades producto de las auditorias internas de seguridad de información. Se integraron en un solo plan las no conformidades de las auditorias 2019 y 2021, con el fin de realizar un seguimiento a la gestión mas eficiente. **Evidencias**: B. Plan de mejoramiento de seguridad de información
		Realizar seguimiento al plan de mejoramiento de seguridad de información	De acuerdo a lo programado en el plan estratégico de seguridad y privacidad de información, esta actividad iniciará en el cuarto trimestre del 2022.

5. Conclusiones.

De acuerdo al Plan Estratégico de Seguridad y Privacidad de la información, establecido para la presente vigencia, durante el primer trimestre se avanzó en un 22% de las actividades propuestas.

Dentro de las estrategias gestionadas se encuentran:

- **Liderazgo de seguridad de la información.** Se avanzó en la revisión y aprobación de la política de seguridad y privacidad de información por parte del Comité Institucional de Gestión y Desempeño y la Oficina Asesora Jurídica.

- **Gestión de riesgos.** Se inició la actualización de los inventarios de activos de información con los delegados de cada uno de los procesos institucionales. Este inventario se tomará como base para llevar a cabo actualización de riesgos de seguridad de información, tomando como referencia aquellos activos catalogados como Críticos y Altos.

- **Concientización, sensibilización y capacitación en seguridad de información.** Se definió el cronograma para dictar las charlas de sensibilización en seguridad a cargo de la Oficina de Tecnología. Se inició con la primera charla dirigida a la SUBAER, sin embargo no se logró la participación de todo el personal de la dependencia. Se inició el envío de los tips seguros que contienen consejos para el cuidado de la información institucional y personal.

- **Medición, revisión y evaluación del SGSI.** Se actualizaron los indicadores de seguridad de información, incluyendo el de participación en actividades de sensibilización y se llevo a cabo la medición de indecentes y riesgos de seguridad de información.

Aprobó: Imelda Muñoz Mancipe

Jefe Oficina de Tecnología

Elaboró: Mayra Alexandra Agudelo Carvajal

Profesional Especializado