USPEC
UNIDAD DE SERVICIOS
PENITENCIARIOS Y CARCELARIOS

Segundo Trimestre de 2022
Presentado Julio 15 de 2022

Informe de gestión trimestral

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	10. Plan de mejoramiento actualizado	Dependencias involucradas - Responsable SGSI (Apoya la gestión)				X
	Realizar seguimiento al plan de mejoramiento de seguridad de información	11. 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	La Dirección General solicitó ajustes al documento de política y de acuerdo a los mismos se llevó a cabo la aprobación de la resolución 000181 de 2022 y publicación en el portal web de la Entidad. Su socialización se llevó a cabo a través de correo institucional. Como actividad adicional de socialización se realizó un guion como insumo para la elaboración de un video. **Evidencias:** A. https://www.uspec.gov.co/media/464 B. Guion socialización política C. Correo de socialización de la política

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.	Durante el segundo trimestre se continuó con la validación de los inventarios de activos logrando avanzar con cada proceso de la siguiente forma: ▪ Gestión Estratégica Organizacional. Revisado y aprobado. ▪ Gestión de la Comunicación Institucional. Revisado, pendiente por aprobación por parte del líder de proceso. ▪ Gestión de Tecnologías de la Información. Revisado y aprobado. ▪ Gestión de Infraestructura. Con corte al 30 de junio, se encontraba por culminar la revisión por parte de la Dirección de Gestión de Infraestructura y aprobación por parte del líder de proceso. ▪ Gestión Contractual. Revisado y aprobado. ▪ Gestión de Suministro de Bienes y Prestación de Servicios. Revisado, pendiente por aprobación por parte del líder de proceso. ▪ Gestión de Atención a Establecimientos de Reclusión. Pendiente por culminar la revisión y aprobación por parte del líder de proceso. ▪ Gestión Financiera. Revisado, pendiente por aprobación por parte del líder de proceso. ▪ Gestión de Atención al Ciudadano. Pendiente por culminar la revisión y aprobación por parte del líder de proceso. ▪ Gestión Documental. Revisado, pendiente por aprobación por parte del líder de proceso. ▪ Gestión de Talento Humano. Revisado, pendiente por aprobación por parte del líder de proceso. ▪ Gestión Jurídica. Pendiente por culminar la revisión y aprobación por parte del líder de proceso. ▪ Evaluación y Control. Revisado y aprobado por parte del líder de proceso. ▪ Gestión de Recursos Físicos y Suministros. Revisado, pendiente por aprobación por parte del líder de proceso.

			Evidencias: A. Inventarios actualizados https://drive.google.com/drive/folders/1F0nlCT5AQGhuPqLtLGoeVL8SqUjwbIF8?usp=sharing
		Aprobar los inventarios de activos actualizados	Se encuentran aprobados por los líderes de proceso, los siguientes inventarios: ▪ Gestión Estratégica Organizacional. ▪ Gestión de Tecnologías de la Información ▪ Evaluación y Control ▪ Gestión Contractual Una vez se culminen todas las aprobaciones por parte de los líderes de proceso y se cuente con el índice de información reservada y clasificado, se procederá a solicitar la aprobación de los artefactos por parte del Comité Institucional de Gestión y Desempeño. **Evidencias:** A. Correos de aprobación
	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.	Durante el segundo trimestre se llevaron a cabo mesas de trabajo virtuales dirigidas por la Oficina de Planeación y el DAFP, con el fin de socializar la nueva metodología de riesgos adoptada por la Entidad. En cuanto a los riesgos de seguridad de información se llevó a cabo la validación de la herramienta a través de la cual se llevará a cabo la identificación de riesgos y adicionalmente se realizó el primer ejercicio de identificación de riesgo con la Dirección de Infraestructura.

			Adicionalmente por parte de la OTEC se realizaron sugerencias de ajuste de la política de administración de riesgos en los aspectos relacionados con seguridad de información. Durante el tercer trimestre se continuará con la gestión para llevar a cabo la actualización de las matrices de riesgos con los procesos institucionales. **Evidencias:** A. Evidencias de participación en las charlas de la OAPLA (Pendiente los soportes por parte de la OAPLA) B. Plantilla de identificación de riesgo. C. Sugerencias ajuste política de seguridad
		Aprobar la matriz de riesgos de seguridad de información	Esta actividad depende de la actualización de los mapas 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	Actividad ejecutada durante el primer trimestre.
		Realizar seguimiento trimestral al plan de comunicación, sensibilización y capacitación en seguridad de información	Se ejecutaron las siguientes actividades: ▪ Se elaboraron piezas con contenidos de tips seguros y correos de alerta y se compartieron con todo el personal de la USPEC a través de correo institucional. ▪ Se realizaron charlas de seguridad con las siguientes dependencias: Subdirección Administrativa, Subdirección Financiera, Subdirección de Construcción y Conservación, Subdirección de

			Seguimiento a la Infraestructura, Dirección de Gestión Contractual. Se obtuvo un porcentaje de participación del 44%, de un total de 321 personas convocadas. ▪ Encuestas de seguridad de información. De acuerdo a las charlas de seguridad realizadas, se compartió con los asistentes una encuesta con el fin de evaluar los conocimientos adquiridos. **<u>Evidencias</u>**: A. Piezas tips seguros B. Evidencias primera charla seguridad de información – SUBAER
		Realizar encuestas para medir el grado de sensibilización del personal de la Entidad.	Tomando como referencia el número total de personas (321) convocadas a la charla de seguridad de información durante el segundo trimestre, solo participó un 5.4% de la encuesta. A continuación se muestra el porcentaje de participación por cada dependencia: ✓ Subdirección Administrativa. 2% ✓ Subdirección Financiera. 10% ✓ Subdirección de Construcción y Conservación. 7% ✓ Subdirección de Seguimiento a la Infraestructura. 8% ✓ Dirección de Gestión Contractual. 0% **<u>Evidencias</u>**: 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. Teniendo en cuenta la gestión realizada durante el segundo trimestre con la Oficina Asesora de Planeación y Desarrollo, se estima avanzar con esta gestión durante el tercer 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. Teniendo en cuenta la gestión realizada durante el segundo trimestre con la Oficina Asesora de Planeación y Desarrollo, se estima avanzar con esta gestión durante el segundo semestre 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 para el segundo trimestre del 11% y un porcentaje acumulado del 30%. A continuación se muestra el detalle de avance por cada dependencia. ✓ Gestión de Contractual. 0% ✓ Gestión Infraestructura. 23% ✓ Gestión de bienes y prestación de servicios. 0% ✓ Gestión de recursos físicos y suministros. 0% ✓ Gestión Talento Humano. 0% ✓ Gestión Jurídica. 20% ✓ Gestión de Atención a Establecimientos de Reclusión. 13% ✓ Gestión de Tecnologías de la Información. 29.5%
	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.	Una vez se lleve a cabo la actualización de riesgos de seguridad de información, se validarán los controles implementados (Anexo A, Norma ISO 27001:2013) a través de métodos de operación por las dependencias involucradas y de esta manera se actualizará la declaración de aplicabilidad.

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 segundo trimestre se revisó la resolución 500 de 2021 con el fin de identificar los elementos que se requieren incluir en los métodos de operación de la Entidad referentes a la gestión de incidentes. Evidencia: A. Revisión resolución 500 de 2021.
Medición, revisión y evaluación del SGSI	Proyecto 1: Gestionar el autodiagnóstico del MSPI	Actualizar el autodiagnóstico MSPI	Se continuó con la actualización del autodiagnóstico del Modelo de seguridad y privacidad de información, evaluando la sección de aspectos técnicos. Se estima culminar la revisión en el tercer trimestre. **Evidencias:** A. Autodiagnóstico MSPI
		Evaluar la necesidad de ajustar los planes de seguridad de información de acuerdo a los resultados del autodiagnóstico	Una vez se finalice la actualización del autodiagnóstico se evaluará la necesidad de incluir otras actividades referentes al fortalecimiento del MSPI.
	Proyecto 2: Gestionar los indicadores de seguridad de información	Actualizar los indicadores de seguridad de información	Actividad ejecutada en el primer trimestre del 2022.
		Realizar seguimiento periódico a los indicadores de seguridad de información	Se realizó seguimiento a los siguientes indicadores: - Gestión de incidentes. (trimestral) 100% - Gestión de vulnerabilidades (semestral). 62% - Porcentaje de avance en el PTR (semestral). 30% En los soportes se encuentra el análisis de cada uno de los indicadores. **Evidencia**:

			A. Análisis de Indicadores
	Proyecto 3: Revisar el avance del Sistema de gestión de seguridad de información.	Realizar el informe semestral de revisión por la dirección.	Se realizó el primer informe de revisión por la Dirección, incluyendo el reporte de los siguientes aspectos: ✓ Estado de las acciones relacionadas con las revisiones previas por parte de la Dirección. ✓ Cambios en los asuntos externos e internos pertinentes al SGSI. ✓ Retroalimentación sobre el desempeño de la seguridad de la información (incluidas las tendencias relativas a no conformidades y acciones correctivas). ✓ Seguimiento y resultados de las mediciones. ✓ Resultados de la auditoría interna realizada en el 2021 ✓ Estado del cumplimiento de los objetivos de seguridad de información. ✓ Retroalimentación de las partes interesadas, resultados de la valoración de riesgos y el estado del plan de tratamiento de riesgos y oportunidades de mejora continua. Durante el tercer trimestre se realizará la gestión para la socialización del informe con la Dirección General y el Comité Institucional de Gestión y Desempeño. **Evidencias:** A. Informe de revisión SGSI
		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: Auditoría externa de seguridad de información	Definir el plan de auditoría y las listas de verificación	Se solicitaron cotizaciones para iniciar el estudio de mercado a través del cual se pretende contratar la auditoría externa de seguridad de información. Con corte al 30 de junio, se recibió una cotización por valor de $25.000.000. **Evidencias:** A. Cotización 1
		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	Actividad ejecutada en el primer trimestre del 2022.
		Realizar seguimiento al plan de mejoramiento de seguridad de información	Se inició el seguimiento del plan de mejoramiento. De un total de 9 no conformidades generadas en la auditoría del 2021, 3 se encuentran en proceso, 4 por iniciar la respectiva gestión y 2 se encuentran subsanados. En cuanto a la auditoría realizada en el 2019, 4 no conformidades se encuentran en proceso de gestión para su subsanación y 8 se encuentran subsanadas. **Evidencia:** A. Plan de mejoramiento y su respectivo seguimiento

5. Conclusiones.

De acuerdo al Plan Estratégico de Seguridad y Privacidad de la información, establecido para la presente vigencia, durante el segundo trimestre se avanzó en un 17% de las actividades propuestas. Para la vigencia se cuenta con un porcentaje de avance del 39%.

Dentro de las estrategias gestionadas se encuentran:

- **Liderazgo de seguridad de la información.** Se avanzó en la aprobación y publicación de la política de seguridad, privacidad de información y seguridad digital en la página web de la Entidad (Resolución 000181 de 2022).

- **Gestión de riesgos.** Se continuó con 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 continuo con las charlas de seguridad de información con la Dirección Administrativa y Financiera, la Dirección de Gestión Contractual y la Dirección de Infraestructura, sin embargo no se obtuvo el porcentaje de participación esperado. A través del correo seguridad.informacion@uspec.gov.co se remitieron tips seguros y correos de alerta que contienen consejos para el cuidado de la información institucional y personal.

- **Medición, revisión y evaluación del SGSI.** Se llevaron a cabo las mediciones de los indicadores de gestión de incidentes, gestión de vulnerabilidades y porcentaje de avance en el plan de tratamiento de riesgos. Se realizó seguimiento al plan de mejoramiento, se inició el estudio de mercado para la contratación de la auditoria externa al SGSI y se elaboró el primer informe de revisión del SGSI.

Aprobó: Imelda Muñoz Mancipe

Jefe Oficina de Tecnología

Revisó: Camilo Alejandro Romero González

Coordinador Grupo Comunicaciones

Elaboró: Mayra Alexandra Agudelo Carvajal

Profesional Especializado