USPEC
UNIDAD DE SERVICIOS
PENITENCIARIOS Y CARCELARIOS

Tercer Trimestre de 2022
Presentado Octubre 12 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 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 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	ACTIVIDADES	PRODUCTOS ESPERADOS	RESPONSABLE	AÑO 2022			
				TRIM 1	TRIM 2	TRIM 3	TRIM 4
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	2. Evidencias de las actividades ejecutadas	Responsable SGSI	X	X	X	X

PROYECTO	ACTIVIDADES	PRODUCTOS ESPERADOS	RESPONSABLE	AÑO 2022			
				TRIM 1	TRIM 2	TRIM 3	TRIM 4
	seguridad de información.	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	ACTIVIDADES	PRODUCTOS ESPERADOS	RESPONSABLE	AÑO 2022			
				TRIM 1	TRIM 2	TRIM 3	TRIM 4
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		

PROYECTO	ACTIVIDADES	PRODUCTOS ESPERADOS	RESPONSABLE	AÑO 2022			
				TRIM 1	TRIM 2	TRIM 3	TRIM 4
	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
		7. Plan de auditoria	Contratista			X	X

PROYECTO	ACTIVIDADES	PRODUCTOS ESPERADOS	RESPONSABLE	AÑO 2022			
				TRIM 1	TRIM 2	TRIM 3	TRIM 4
Proyecto 4: Auditoria externa de seguridad de información	Definir el plan de auditoria y las listas de verificación	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	La política se aprobó en el segundo trimestre del 2022.

ESTRATEGIA	PROYECTO	ACTIVIDAD	EJECUCIÓN
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.	Se culminó la actualización de los inventarios de activos de información para 14 procesos institucionales. En el caso de los procesos Gestión interinstitucional e Investigación y aprendizaje para la gestión penitenciaria, no se identificaron activos teniendo en cuenta que no cuentan con documentación estructurada (De acuerdo a concepto brindado por la Oficina Asesora de Planeación) **Evidencias:** A. Inventarios de activos por proceso B. Correo de la OAPLA https://drive.google.com/drive/folders/1kPzfWS8f0rKpT8QdhtFkC94co-RHQdNx?usp=sharing
		Aprobar los inventarios de activos actualizados	Se aprobaron por los líderes de proceso, los siguientes inventarios: ✓ Gestión de la comunicación institucional ✓ Gestión de suministro de bienes y prestación de servicios ✓ Gestión de atención a establecimientos ✓ Gestión de infraestructura ✓ Gestión jurídica ✓ Gestión de talento humano ✓ Gestión de atención al ciudadano ✓ Gestión documental ✓ Gestión financiera ✓ Gestión de recursos físicos y suministros **Evidencias:** A. Correos de aprobación por parte de cada líder de proceso.

ESTRATEGIA	PROYECTO	ACTIVIDAD	EJECUCIÓN
			https://drive.google.com/drive/folders/1_jzKf8e4VyW2D5LqfuIQFx02-_di7nzn?usp=sharing
	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 tercer trimestre la Oficia de Tecnología llevó a cabo la validación de la declaración de aplicabilidad de la Entidad con el fin de determinar los controles de seguridad de información que se requieren documentar y/o implementar y así mismo se evaluaron los posibles riesgos de los procesos de acuerdo a la responsabilidad en la implementación de controles establecidos en el Anexo A de la Norma ISO 27001:2013. **Evidencias:** A. Evaluación de riesgos por procesos VS controles https://docs.google.com/spreadsheets/d/1Bd2EPQ-QlsGYQX-Jq1Ex7Z4s6XBv4_M6/edit?usp=sharing&ouid=105627553757337286070&rtpof=true&sd=true
		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,	Se ejecutaron las siguientes actividades:

ESTRATEGIA	PROYECTO	ACTIVIDAD	EJECUCIÓN
		sensibilización y capacitación en seguridad de información	▪ Se elaboraron y compartieron a través de correo institucional, piezas con contenidos de tips seguros y alertas de seguridad de información e historias de la vida real (estas últimas relacionadas con los intentos de vulneración de información personal que algunos usuarios han reportado a la OTEC) con el fin de concientizar al personal de la USPEC frente a las amenazas actuales de robo de información. ▪ Se compartió invitación a todos los usuarios de la Entidad para participar en charla de seguridad de información brindada por el Ministerio de Justicia ▪ De acuerdo a las inquietudes remitidas por los usuarios de la Entidad frente a posibles intentos de robo de información o estafas, se han aclarado las dudas a través de correo. **Evidencias**: A. Piezas tips seguros, alertas e historias de la vida real B. Invitación charla seguridad de información – MinJusticia C. Respuesta a inquietudes de usuarios https://drive.google.com/drive/folders/19awiMcesHWuhK0g7z5CKIjbZkKJ60ENL?usp=sharing
		Realizar encuestas para medir el grado de sensibilización del	De acuerdo al cronograma establecido inicialmente, esta actividad se finalizará en el cuarto trimestre del año.

ESTRATEGIA	PROYECTO	ACTIVIDAD	EJECUCIÓN
		personal de la Entidad.	
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	Durante el tercer trimestre la OTEC trabajó en el análisis de los controles de la Norma ISO 27001:2013, con el fin de identificar posibles riesgos para los procesos de la Entidad, con esta información se espera para el cuarto trimestre llevar a cabo la actualización de las matrices de riesgos y por ende de los planes de tratamiento de riesgos. **Evidencias**: A. Análisis de posibles riesgos de seguridad (Declaración de aplicabilidad) https://docs.google.com/spreadsheets/d/1Bd2EPQ-QlsGYQX-Jq1Ex7Z4s6XBv4_M6/edit?usp=sharing&ouid=105627553757337286070&rtpof=true&sd=true
		Aprobar el plan de tratamiento de riesgos de seguridad de información	Esta actividad depende de la anterior, una vez se cuente con los planes de tratamiento de riesgos actualizados se solicitará su aprobación a cada uno de los líderes de proceso.
		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, cabe mencionar que este plan es el aprobado a inicios de la presente vigencia. En conclusión, de acuerdo a la información reportada por cada una de las dependencias, se obtuvo un porcentaje de avance del 7%, para un porcentaje acumulado en la vigencia del 30%.

ESTRATEGIA	PROYECTO	ACTIVIDAD	EJECUCIÓN
			Evidencia: ✓ Plan de tratamiento de riesgos de seguridad de información
	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.	Se inició la actualización de la declaración de aplicabilidad y se identificaron necesidades de implementación de controles, así como las dependencias responsables de llevar a cabo la gestión requerida. Se encuentra pendiente evaluar las acciones de implementación de algunos controles técnicos entre los que se encuentran los dominios de Control de acceso, equipos, seguridad de las operaciones y las comunicaciones y registro y seguimiento. **Evidencias**: A. Declaración de aplicabilidad https://docs.google.com/spreadsheets/d/1Bd2EPQ-QlsGYQX-Jq1Ex7Z4s6XBv4_M6/edit?usp=sharing&ouid=105627553757337286070&rtpof=true&sd=true
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	Se actualizó el procedimiento de gestión de eventos e incidentes de seguridad de información y se remitió el 28 de septiembre a través de correo a la OAPLA para revisión y observaciones. **Evidencias**: A. Borrador de procedimiento B. Correo de envío a la OAPLA.

ESTRATEGIA	PROYECTO	ACTIVIDAD	EJECUCIÓN
			https://drive.google.com/drive/folders/1o36Yka-0tTSo9Rjf7rI4_fX0H4orqK8K?usp=sharing
Medición, revisión y evaluación del SGSI	Proyecto 1: Gestionar el autodiagnóstico del MSPI	Actualizar el autodiagnóstico MSPI	Se culminó la actualización del autodiagnóstico del Modelo de seguridad y privacidad de información, herramienta establecida por MINTIC. **Evidencias:** A. Autodiagnóstico MSPI https://drive.google.com/drive/folders/17Vz6I06VxAJOIwwZkfK3-cQ118l9n6ut?usp=sharing
		Evaluar la necesidad de ajustar los planes de seguridad de información de acuerdo a los resultados del autodiagnóstico	La evaluación del autodiagnóstico se culminó en el tercer trimestre al igual que se avanzó en la actualización de la declaración de aplicabilidad. A través de estos insumos se determinaron las necesidades en cuanto a la implementación de controles de seguridad que se requieren mejorar para contribuir con la mejora continua del SGSI. Adicionalmente la información aquí recopilada permitirá llevar a cabo la actualización de las matrices de riesgos de seguridad de información por proceso y el respectivo plan de tratamiento de riesgos. **Evidencias**: A. Declaración de aplicabilidad https://docs.google.com/spreadsheets/d/1Bd2EPQ-QlsGYQX-Jq1Ex7Z4s6XBv4_M6/edit?usp=sharing&ouid=105627553757337286070&rtpof=true&sd=true

ESTRATEGIA	PROYECTO	ACTIVIDAD	EJECUCIÓN
	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. Durante el tercer trimestre no se reportaron incidentes de seguridad de información. ✓ Gestión de vulnerabilidades. Este indicador es semestral, el próximo corte es el 31/12/2022. ✓ Gestión de riesgos de seguridad. Durante el trimestre se avanzó en un 7% de implementación del plan de tratamiento de riesgos, de acuerdo al reporte remitido por cada una de las dependencias. Cabe mencionar que solamente reportaron información 4 procesos: Gestión de atención a establecimientos de reclusión, Gestión de infraestructura, Gestión Jurídica y Gestión de tecnologías de la información. **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.	El segundo informe se encuentra programado para el cuarto trimestre del 2022.
		Tomar decisiones relevantes para la mejora continua del SGSI	De acuerdo a la revisión de los procedimientos que hacen parte del SGSI se determinó la necesidad de actualizar las actividades para llevar a cabo la gestión de habilitación y deshabilitación de cuentas de usuario, adicionando a la gestión el formato de paz y salvo a través del cual se busca mantener la trazabilidad de los usuarios que se retiran de la entidad. Adicionalmente se determinó la necesidad de ajustar el

ESTRATEGIA	PROYECTO	ACTIVIDAD	EJECUCIÓN
			procedimiento de gestión de medios removibles, para facilitar el manejo de información institucional requerida por los usuarios a través de estos medios. En tal sentido durante el tercer trimestre se llevó a cabo la actualización de dichos documentos y se remitieron a la OAPLA para revisión.
	Proyecto 4: Auditoría externa de seguridad de información	Definir el plan de auditoría y las listas de verificación	Se realizaron los estudios previos para la contratación de la auditoria de seguridad de información y se remitieron para revisión a la Dirección de Gestión Contractual el 6 de septiembre de 2022 a través del memorando I-2022-026020. Sin embargo, con corte al 30 de septiembre no se contaba con notificación al respecto por parte de dicha dependencia. **Evidencias:** A. Memorando I-2022-026020 – Estudio previo
		Ejecutar el plan de auditoria	Esta actividad depende de la contratación de la Auditoría de seguridad, con corte al 30 de septiembre el estudio previo se encontraba en revisión por parte de la Dirección de Gestión Contractual.
	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	El siguiente avance de esta actividad se encuentra programada para el cuarto trimestre

5. Conclusiones.

De acuerdo al Plan Estratégico de Seguridad y Privacidad de la información, establecido para la presente vigencia, durante el tercer trimestre se avanzó en un 18% de las actividades propuestas.

Dentro de las estrategias gestionadas se encuentran:

- **Gestión de riesgos.** Se culminó la actualización de los inventarios de activos de información con los delegados de cada uno de los procesos institucionales y se procedió con la aprobación de los mismos por cada uno de los líderes de proceso. Adicionalmente por parte de la OTEC se identificaron aquellos controles de la Norma ISO 27001:2013 que requieren mayor gestión por parte de los diferentes procesos institucionales determinando así posibles riesgos de seguridad de información. Esta información se tomará como referencia para llevar a cabo actualización del mapa de riesgos de seguridad de información.

- **Concientización, sensibilización y capacitación en seguridad de información.** Se continuó con el envío de alertas, tips seguros e historias de seguridad de la vida real a través de correo institucional dirigidos a todo el personal de la entidad. Así mismo se remitió la invitación realizada por el Ministerio de Justicia para participar en una charla de seguridad de información.

- **Implementación del plan de tratamiento de riesgos de seguridad de información.** Se inició la actualización de declaración de aplicabilidad la cual contiene la evaluación de los controles de seguridad de información referenciados en la Norma ISO 27001:2013. Se avanzó en un 7% de implementación del plan de tratamiento de riesgos de seguridad de información establecido a inicios de la vigencia.

- **Gestión de incidentes.** Se actualizó el procedimiento de gestión de eventos e incidentes de seguridad de información de acuerdo a los lineamientos establecidos en la Resolución 500 de 2021 y se remitió a la OAPLA para revisión.

- **Medición, revisión y evaluación del SGSI.** Se culminó la actualizaron del autodiagnóstico de seguridad de información, se realizó el seguimiento a los indicadores de seguridad de información, se avanzó en la construcción de los estudios previos para la contratación de la auditoría de seguridad de información y se remitieron a la Dirección de Gestión Contractual el 6 de septiembre, sin embargo con corte al 30 de septiembre no se habían recibido observaciones por parte de dicha dependencia, lo que ha generado retrasos en la ejecución de las actividades contempladas en el presente plan.

Aprobó: Imelda Muñoz Mancipe

Jefe Oficina de Tecnología

Elaboró: Mayra Alexandra Agudelo Carvajal

Profesional Especializado