USPEC
UNIDAD DE SERVICIOS
PENITENCIARIOS Y CARCELARIOS

Cuarto Trimestre de 2022
Presentado Diciembre 20 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	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.
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 actualización de los inventarios de activos finalizó en el tercer trimestre del 2022.

	institucionales, de acuerdo a la metodología establecida por la Entidad.	Aprobar los inventarios de activos actualizados	Cada uno de los líderes de proceso realizó la aprobación de su inventario de activos de información a través de correo en el tercer trimestre del 2022.
	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 4 trimestre se llevó a cabo la actualización de los riesgos de seguridad de información, sus controles y respectivos planes de tratamiento con cada uno de los delegados de los procesos. **Evidencias:** A. Matrices de riesgos por proceso
		Aprobar la matriz de riesgos de seguridad de información	Al finalizar el semestre se realizará la aprobación por parte del Comité Institucional de Gestión y Desempeño del mapa de riesgos institucional, incluidos los riesgos de seguridad de información. **Evidencias:** A. Acta De aprobación del Comité Institucional de Gestión y Desempeño (A cargo de la Oficina Asesora de Planeación)
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 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 realizó ejercicio controlado de phishing, posterior a su ejecución se presentaron los siguientes resultados: • 645 envíos exitosos a cuentas @uspec.gov.co • 427 usuarios leyeron y/o abrieron el mensaje • 213 usuarios no leyeron y/o abrieron el mensaje • 183 usuarios hicieron clic en enlace "Inscribirse aquí" • 1 usuario se desuscribió de la lista de envíos • 0 usuarios reportes spam ▪ Se programaron charlas de seguridad de información con el fin de reforzar los conocimientos de los usuarios frente a las amenazas del ciberespacio. Sin embargo de un total 568 invitaciones enviadas, solo participaron 75 usuarios entre funcionarios y contratistas. **Evidencias**: A. Piezas tips seguros, alertas e historias de la vida real B. Invitación charla seguridad de información C. Memorando invitando a charla de sensibilización D. Informe de phishing https://drive.google.com/drive/folders/16Nz2W19NYh12hKik2IC1IX58tdS_KD46?usp=share_link

		Realizar encuestas para medir el grado de sensibilización del personal de la Entidad.	Se envió encuesta a todos los funcionarios y contratistas de la Entidad con el fin de evaluar la conciencia que se tiene frente a las amenazas del ciberespacio. **Evidencias**: A. Invitación para participar en encuesta de seguridad de información https://drive.google.com/file/d/1LCuh_8fqNjGRtbVy0hhKX8aMmeErw124/view?usp=share_link
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	Se llevó a cabo la actualización del plan de tratamiento de riesgos tomando como referencia la información definida por cada uno de los procesos que cuentan con riesgos de seguridad de información. **Evidencias**: A. Plan de tratamiento de riesgos de seguridad de información actualizado.
		Aprobar el plan de tratamiento de riesgos de seguridad de información	Al finalizar el semestre se realizará la aprobación por parte del Comité Institucional de Gestión y Desempeño del plan de tratamiento de riesgos de seguridad de información. **Evidencias:** A. Acta De aprobación del Comité Institucional de Gestión y Desempeño (A cargo de la Oficina Asesora de Planeación)

		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 para el trimestre del 9.3% y un acumulado para la vigencia de 45.7%. **Evidencia:** A. Informe de ejecución del 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 llevó a cabo la actualización de la declaración de aplicabilidad de acuerdo a los controles implementados durante la vigencia anterior por los procesos involucrados. **Evidencias**: A. Declaración de aplicabilidad https://docs.google.com/spreadsheets/d/1OByGM4juw4-21wx-tmr_Sxb-fZ4Ajy1I/edit?usp=share_link&ouid=105627553757337286070&rtpof=true&sd=true
Gestión de incidentes	Proyecto 1: Llevar a cabo la gestión de incidentes conforme a lo establecido	Actualizar el procedimiento de gestión de eventos e incidentes de seguridad de información	Se aprobó, publicó y socializó a través de correo la actualización del procedimiento TI-PR-04 Gestión de eventos e incidentes de seguridad de información. **Evidencias**:

	en la Resolución 500 de 2021.		https://mipgestion.uspec.gov.co/files/mod_documentos/documentos/TI-PR-004/TI-PR-004%20Gesti%C3%B3n%20de%20Eventos%20e%20Incidentes%20de%20Seguridad%20de%20la%20Informaci%C3%B3n_V3_copia_controlada.pdf
Medición, revisión y evaluación del SGSI	Proyecto 1: Gestionar el autodiagnóstico del MSPI	Actualizar el autodiagnóstico MSPI	En el tercer trimestre se culminó la actualización del autodiagnóstico del Modelo de seguridad y privacidad de información
		Evaluar la necesidad de ajustar los planes de seguridad de información de acuerdo a los resultados del autodiagnóstico	Se llevó a cabo la actualización del plan de tratamiento de riesgos tomando como referencia los resultados del autodiagnóstico y la evaluación de la declaración de aplicabilidad. **Evidencias**: A. Plan tratamiento de riesgos
	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 se reportó y solucionó un incidente de seguridad de información asociado con la disponibilidad de información del servidor de archivos, se llevó a cabo su respectivo análisis. ✓ Gestión de vulnerabilidades. Teniendo en cuenta que no avanzó en la gestión de vulnerabilidades no fue posible evaluar este indicador.

			Gestión de riesgos de seguridad. De acuerdo a las actividades ejecutadas y reportadas por los procesos institucionales, durante el cuarto trimestre se avanzó en un 9.3% y un porcentaje acumulado para el año de 45.7%. En conclusión, durante la presente vigencia los procesos avanzaron vigencia de la siguiente forma: ▪ Gestión de Contractual. 0% ▪ Gestión Infraestructura. 37% ▪ Gestión de bienes y prestación de servicios. 0% ▪ Gestión de recursos físicos y suministros. 0% ▪ Gestión Talento Humano. 100% ▪ Gestión Jurídica. 70% ▪ Gestión de Atención a Establecimientos de Reclusión. 79% ▪ Gestión de Tecnologías de la Información. 80% **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 segundo informe de revisión por la dirección incluyendo los siguientes elementos: ▪ 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. **Evidencias**: A. Informe de revisión por la dirección
		Tomar decisiones relevantes para la mejora continua del SGSI	Se llevó a cabo la actualización del mapa de riesgos institucional, incluyendo los riesgos de seguridad de información y los respectivos planes de tratamiento que permitirán durante el 2023 monitorear controles para la mitigación de riesgos que afecten la confidencialidad, integridad y/o disponibilidad de la información institucional. Sin embargo, se encuentra pendiente la revisión del informe de revisión por la dirección como insumo para la toma de decisiones por parte de la Alta Dirección., labor que se prevé ejecutar a inicios de la siguiente vigencia.

<table>
<tr>
<td rowspan="2"></td>
<td rowspan="2">Proyecto 4: Auditoría externa de seguridad de información</td>
<td>Definir el plan de auditoría y las listas de verificación</td>
<td rowspan="2">El 6 de septiembre a través del memorando I-2022-026020, se remitió a la Dirección de Gestión Contractual la solicitud de revisión de estudios previos para contratar la auditoria interna de seguridad de información bajo los requisitos de la Norma ISO 27001:2013. Posteriormente de acuerdo a los ajustes solicitados por la DIGECO, el 11 de octubre a través del memorando I-2022-026675, la OTEC radicó nuevamente los estudios previos ajustados y matriz de riesgos.

El 18 de octubre se realizó la publicación del proceso en la plataforma del SECOP II, y se realizó la designación del comité evaluador por parte de la Dirección de Gestión Contractual, asignando al personal de su dependencia para llevar a cabo la respectiva gestión. Sin embargo, por parte de la OTEC, se apoyó de manera proactiva el proceso de evaluación.

El 11 de noviembre se generó la resolución 000608, a través de la cual se indicó que el proceso quedaba desierto porque ninguna de las dos ofertas presentadas cumplió con los requisitos técnicos establecidos.

En tal sentido, y teniendo en cuenta el tiempo requerido para generar un nuevo proceso, por parte de la Jefatura de la Oficina de Tecnología, se tomó la decisión de no continuar con la gestión para ejecutar la auditoria interna de seguridad de información durante la presente vigencia.

<u>Evidencias:</u>

A. Memorando I-2022-026020 del 6 de septiembre
B. Memorando I-2022-026675 del 11 de octubre
C. Resolución 000608 de 2022</td>
</tr>
<tr>
<td>Ejecutar el plan de auditoria</td>
</tr>
</table>

	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 realizó seguimiento al plan de mejoramiento de seguridad de información, de acuerdo a la gestión realizada durante la presente vigencia, se generaron los siguientes resultados: **Evidencias:** A. Seguimiento plan de mejoramiento https://docs.google.com/spreadsheets/d/107W5KdPIYc8WI7GUkMi6fWpUdxmBiMcH/edit?usp=share_link&ouid=105627553757337286070&rtpof=true&sd=true

5. Conclusiones.

De acuerdo al Plan Estratégico de Seguridad y Privacidad de la información, establecido para la presente vigencia, durante el cuarto trimestre se avanzó en un 34% de las actividades propuestas y para el 2022 se obtuvo un 91% en la ejecución total del plan propuesto. Dentro de las estrategias desarrolladas en su totalidad se encuentran:

- ✓ Liderazgo de seguridad de la información.
- ✓ Gestión de riesgos.
- ✓ Concientización, sensibilización y capacitación en seguridad de información.

En cuanto a la estrategia Medición, revisión y evaluación del SGSI, se avanzó en la actualización del autodiagnóstico de SGSI, actualización y seguimiento a indicadores, informes de revisión por la dirección, actualización y seguimiento a plan de mejoramiento. Como actividades pendientes por culminar se encuentra la auditoria en seguridad de información, a pesar de la gestión realizada por la Oficina de Tecnología para contratar este proceso, finalmente salió desierto porque los proponentes que se presentaron no realizaron no subsanaron oportunamente y el tiempo faltante para finalizar la vigencia no permitía retomar nuevamente el proceso. Se planea retomar esta actividad en la vigencia 2023.

Aprobó: Imelda Muñoz Mancipe
Jefe Oficina de Tecnología

Elaboró: Mayra Alexandra Agudelo Carvajal
Profesional Especializado

Revisó: Camilo Alejandro Romero González
Coordinador Grupo Comunicaciones