USPEC
UNIDAD DE SERVICIOS
PENITENCIARIOS Y CARCELARIOS

Segundo Trimestre de 2023
Presentado Julio 12 de 2023

Informe de gestión trimestral

Plan Estratégico de Seguridad y Privacidad de Información

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 2023.

2. ESTRATEGIA DE SEGURIDAD DIGITAL

La USPEC definió su estrategia de seguridad digital a través de las siguientes 7 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:

3. SEGUIMIENTO:

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 2023				SEGUIMIENTO 2 TRIMESTRE	
				TRIM 1	TRIM 2	TRIM 3	TRIM 4	DESCRIPCIÓN DEL AVANCE	PORCENTAJE DE AVANCE
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	No se realizaron avances durante el trimestre. La actividad se encuentra programada para el 4 trimestre.	0%
Eje: Gestión de riesgos									
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	1. Matriz de riesgos de seguridad digital actualizada.	Responsable SGSI(Apoya la gestión) Todas las Dependencias				X	Los riesgos de seguridad de información se actualizaron durante el primer trimestre del 2023, teniendo en cuenta las mesas de trabajo adelantadas con los diferentes procesos institucionales. El resultado se encuentra publicado en el portal	0%

	riesgos de seguridad de información por cada proceso institucional							web institucional, cumpliendo así con el 100% de la actividad. https://uspec.gov.co/gestion-institucional/riesgos El reporte de esta actividad se realizó en el primer trimestre.	
	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	A través del comité institucional de gestión y desempeño se aprobó durante el primer trimestre el plan de tratamiento de riesgos de seguridad de información de acuerdo a la gestión adelantada con los procesos institucionales, cumpliendo así con el 100% de la actividad. El reporte de esta actividad se realizó en el primer trimestre.	0%
Eje: Concientización, sensibilización y capacitación									
Proyecto 3: Gestionar el plan de sensibilización, capacitación y comunicación en seguridad	Actualizar el plan de sensibilización, capacitación y comunicación en seguridad	1. Plan de Sensibilización, comunicación y capacitación actualizado.	Responsable SGSI	X				Durante el primer trimestre se realizó la actualización del plan de sensibilización, capacitación y comunicación en seguridad de información, cumpliendo así con el 100% de la actividad. En dicho trimestre se realizó el reporte.	0%

de información.	de información								
	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	Durante el trimestre se realizaron las siguientes actividades definidas dentro de las estrategias del plan de sensibilización, comunicación y capacitación: * **Tips de seguridad de información.** Durante el trimestre se enviaron correos informativos a todos los usuarios de la Entidad con información sobre correos maliciosos. * **Usuario SGSI** Según los reportes remitidas por los usuarios de la Entidad frente a posibles eventos de seguridad de información, se otorgó durante el trimestre el reconocimiento al usuario SGSI. * **Charlas de sensibilización**	25%
		3. Seguimiento de actividades	Responsable SGSI						

								• Charla de ciberseguridad, dirigida por el proveedor del servicio de correo, Xertica. Aunque la invitación se envió al total de usuarios de la Entidad (437), solo se logró un porcentaje de participación del 15%, de acuerdo a la información recopilada en los soportes de asistencia. • Charla sobre detección de correos maliciosos con usuarios específicos. • Charla sobre protección de datos personales realizada por la Superintendencia de Industria y Comercio **Inducción General.** • Participación en la jornada de inducción impartida a todos los usuarios de la Entidad en la cual se dieron a conocer directrices generales sobre seguridad de información. **Ejercicio de Phishing** Se llevó a cabo un ejercicio controlado de phishing, de 513 mensajes enviados a los buzones de correo institucional, 78	

								personas abrieron el correo y dieron click en el enlace.	
	Realizar encuestas para medir el grado de sensibilización del personal de la Entidad.	4. Resultado de las encuestas de medición	Responsable SGSI		X		X	Se realizó encuesta de seguridad de información entre el personal que participó en la charla de ciberseguridad, con el fin de medir los conocimientos adquiridos en la misma. En conclusión de un total de 437 invitaciones que se enviaron para participar en la charla, solo participaron 67 usuarios y de ellos solo 50 contestaron la encuesta.	50%
Eje: Implementación del plan de tratamiento de riesgos de seguridad de información									
Proyecto 4: Gestionar el plan de tratamiento de riesgos de seguridad de información.	Realizar seguimiento trimestral al plan de tratamiento de riesgos de seguridad de información	1. 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	Se efectuó seguimiento a las actividades ejecutadas del plan de tratamiento de riesgos a cargo de cada una de las dependencias que cuentan actualmente con riesgos de seguridad de información. En conclusión, se obtuvieron los siguiente resultados: ✓ Gestión de Contractual 76% ✓ Gestión Infraestructura 38% ✓ Gestión de recursos Físicos y Suministros 0%	25%

								✓ Gestión de Atención al Ciudadano 0% ✓ Gestión Talento Humano 44% ✓ Gestión Jurídica 58% ✓ Gestión Documental 50% ✓ Gestión Financiera 27% ✓ Gestión de Tecnologías de la Información 30%	
Eje: Gestión de incidentes									
Proyecto 5: Llevar a cabo la gestión de incidentes conforme a lo establecido en el Procedimiento de gestión de eventos e incidentes de seguridad de información	Realizar el análisis de los eventos y/o incidentes de seguridad de información, de acuerdo al reporte realizado por los usuarios.	1. Análisis de indicador de gestión de incidentes	Responsable SGSI - Equipo de gestión de incidentes				X	Se realizó el análisis de los eventos presentados durante el trimestre de acuerdo a la información establecida en el formato Gestión de eventos e incidentes de seguridad de información. En general, se presentaron un total de 37 correos reportados por los usuarios, se ejecutaron un total de 4 archivos. EXE que contenían malware y se tomaron las medidas pertinentes con el fin de no generar afectación en la plataforma tecnológica. Adicionalmente, se remitieron al CSIRT Gobierno, el listado de correos maliciosos recibidos durante el segundo trimestre, de	50%
		2. Soportes de análisis de eventos y/o incidentes					X		

								acuerdo a los reportes enviados por los usuarios al correo seguridad.informacion@uspec.gov.co	
Eje: Medición, revisión y evaluación del SGSI									
Proyecto 6: Gestionar los indicadores de seguridad de información	Actualizar los indicadores de seguridad de información	1. Indicadores actualizados	Responsable SGSI	X				En el primer trimestre se llevó a cabo la gestión para actualizar los indicadores requeridos.	25%
	Realizar seguimiento periódico a los indicadores de seguridad de información	2. Reporte de seguimiento a indicadores	Responsable SGSI	X	X	X	X	Se llevó a cabo el seguimiento de los indicadores de acuerdo a lo programado para el trimestre obteniendo los siguientes resultados: ✓ Indicador avance PTR: 36% ✓ Indicador gestión de incidentes: 67% ✓ Indicador de participación. 15%	25%
Proyecto 7: Revisar el avance del Sistema de gestión de seguridad de información.	Realizar el informe semestral de revisión por la dirección.	1. Informe semestral de revisión por la dirección.	Responsable SGSI		X		X	Se realizó el informe de revisión por la dirección, incluyendo los siguientes temas: • Estado de las acciones relacionadas con las revisiones previas por parte de la Dirección. • Cambios en los asuntos externos e internos pertinentes al SGSI.	50%

								• Retroalimentación sobre el desempeño de la seguridad de la información • Oportunidades de mejora continua.	
Proyecto 8: Auditoria externa de seguridad de información	Definir el plan de auditoria y las listas de verificación	1. Plan de auditoria	Contratista			X	X	No se realizaron avances durante el trimestre. La actividad se encuentra programada para el 3er y 4to trimestre.	0%
		2. Listas de verificación	Contratista			X	X	No se realizaron avances durante el trimestre. La actividad se encuentra programada para el 3er y 4to trimestre.	0%
	Ejecutar el plan de auditoria	3. Informe de auditoria	Contratista			X	X	No se realizaron avances durante el trimestre. La actividad se encuentra programada para el 3er y 4to trimestre.	0%
Proyecto 9: Gestionar el plan de mejoramiento de seguridad de información.	Actualizar el plan de mejoramiento de seguridad de información	1. Plan de mejoramiento actualizado	Dependencias involucradas - Responsable SGSI (Apoya la gestión)				X	La siguiente actualización del plan de mejoramiento depende de la ejecución de la auditoria de seguridad de información programada para la presente vigencia.	0%
	Realizar seguimiento al plan de	2. Seguimiento	Responsable SGSI		X		X	Se realizó seguimiento al plan de mejoramiento producto de la	50%

	mejoramiento de seguridad de información	al plan de mejoramiento						auditoria de seguridad realizada en el mes de enero, en conclusión: ✓ Gestión de Infraestructura, Gestión Documental, Gestión Jurídica y Grupo de Talento Humano continúan ejecutando las actividades propuestas. ✓ Gestión de Tecnologías de la Información, Gestión de Suministro de Bienes y Prestación de Servicios, Gestión Contractual, Grupo de Administración de Personal dieron cumplimiento a las actividades definidas. ✓ Evaluación de la Gestión Institucional y Gestión de Recursos Físicos y Suministros, no realizaron el reporte de información.	
Eje: Relación con proveedores de seguridad digital									
Proyecto 10: Implementar lineamientos para la gestión con los	Definir los lineamientos para llevar a cabo la gestión de los	1.Lineamientos para la gestión de proveedores de TI	Oficina de Tecnología				X	Se publicó en el software MIPGESTION el documento TI-GU-004 Guía de gestión de proveedores de TI y se socializó a través de correo institucional.	50%

proveedores de TI.	proveedores de TI, de acuerdo a lo establecido a través de la Resolución 500 de 2021							Teniendo en cuenta que este documento hace parte de otros planes de la Oficina de Tecnología, se adelantó la gestión, cabe mencionar que en el reporte del primer trimestre para esta actividad se había registrado un porcentaje de avance del 50% y durante el segundo trimestre se finalizó la gestión.	

4. 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 25% de las actividades propuestas, logrando un porcentaje de avance para la vigencia del 50%.

A continuación se muestran los porcentajes de avance durante el primer y segundo trimestre por cada uno de los ejes:

PROYECTO	ACTIVIDADES	PORCENTAJE DE AVANCE 1 TRIMESTRE	PORCENTAJE DE AVANCE 2 TRIMESTRE	PORCENTAJE ACUMULADO 2023
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	0%	0%	0%
Eje: Gestión de riesgos				
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 proceso institucional.	100%	0%	100%
	Aprobar la matriz de riesgos de seguridad de información	100%	0%	100%
Eje: Concientización, sensibilización y capacitación				
Proyecto 3: Gestionar el plan de sensibilización, capacitación y comunicación en seguridad de información.	Actualizar el plan de sensibilización, capacitación y comunicación en seguridad de información	100%	0%	100%
	Realizar seguimiento trimestral al plan de comunicación, sensibilización y capacitación en	25%	25%	50%

	seguridad de información.			
	Realizar encuestas para medir el grado de sensibilización del personal de la Entidad.	0%	50%	50%
Eje: Implementación del plan de tratamiento de riesgos de seguridad de información				
Proyecto 4: Gestionar el plan de tratamiento de riesgos de seguridad de información.	Realizar seguimiento trimestral al plan de tratamiento de riesgos de seguridad de información	25%	25%	50%
Eje: Gestión de incidentes				
Proyecto 5: Llevar a cabo la gestión de incidentes conforme a lo establecido en el Procedimiento de gestión de eventos e incidentes de seguridad de información	Realizar el análisis de los eventos y/o incidentes de seguridad de información, de acuerdo al reporte realizado por los usuarios.	0%	50%	50%
Eje: Medición, revisión y evaluación del SGSI				
Proyecto 6: Gestionar los indicadores de seguridad de información	Actualizar los indicadores de seguridad de información	25%	25%	50%
	Realizar seguimiento periódico a los indicadores de seguridad de información	25%	25%	50%
Proyecto 7: Revisar el avance del Sistema de gestión de seguridad de información.	Realizar el informe semestral de revisión por la dirección.	0%	50%	50%
Proyecto 8: Auditoria externa de seguridad de información	Definir el plan de auditoria y las listas de verificación	0%	0%	0%
		0%	0%	0%
	Ejecutar el plan de auditoria	0%	0%	0%
Proyecto 9: Gestionar el plan de mejoramiento	Actualizar el plan de mejoramiento de seguridad de información	50%	0%	50%

de seguridad de información.	Realizar seguimiento al plan de mejoramiento de seguridad de información	0%	50%	50%
Eje: Relación con proveedores de seguridad digital				
Proyecto 10: Implementar lineamientos para la gestión con los proveedores de TI.	Definir los lineamientos para llevar a cabo la gestión de los proveedores de TI, de acuerdo a lo establecido a través de la Resolución 500 de 2021	50%	50%	100%
Total avance		29,4%	21%	50,0%
Reportado plan de acción		25%	25%	50,0%

Dentro de las estrategias trabajadas en el trimestre se encuentran:

- ✓ Concientización, sensibilización y capacitación en seguridad de información.
- ✓ Implementación del plan de tratamiento de riesgos de seguridad de información
- ✓ Gestión de incidentes
- ✓ Medición, revisión y evaluación del SGSI
- ✓ Relación con proveedores de seguridad digital

Aprobó: Imelda Muñoz Mancipe

Jefe Oficina de Tecnología

Elaboró: Mayra Alexandra Agudelo Carvajal

Profesional Especializado

USPEC
UNIDAD DE SERVICIOS
PENITENCIARIOS Y CARCELARIOS

INFORME DE SEGUIMIENTO AL PLAN DE ACCIÓN – TRIMESTRE II
OFICINA DE TECNOLOGÍA
Plan Estratégico de Seguridad y Privacidad de Información