UNIDAD DE SERVICIOS PENITENCIARIOS Y CARCELARIOS - USPEC

INFORME DE EJECUCIÓN DEL PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE INFORMACIÓN - PESPI

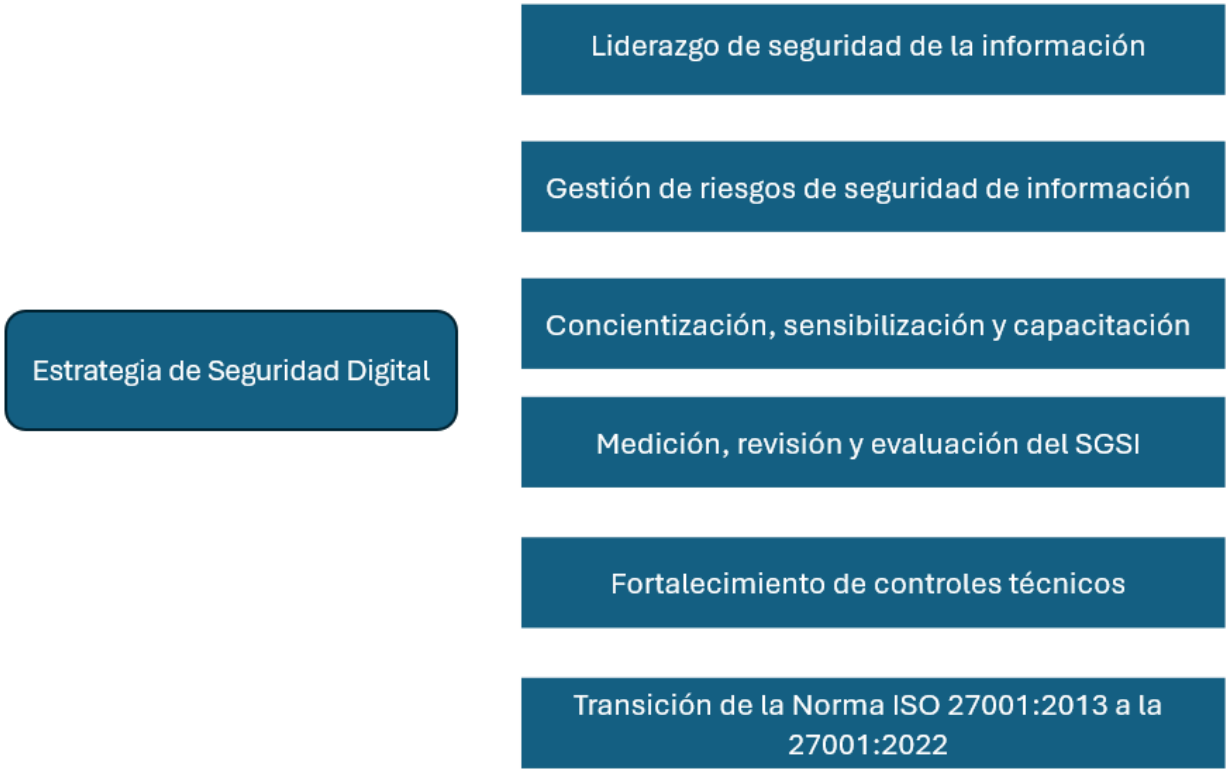
BOGOTÁ D.C., 07 DE OCTUBRE 2024

TERCER TRIMESTRE 2024

1. OBJETIVO

Realizar seguimiento por parte de la Oficina de Tecnología y el Oficial de Seguridad de Información a la implementación del Plan Estratégico de Seguridad y Privacidad de Información, de acuerdo a las actividades establecidas en cada una de las estrategias propuestas para la vigencia 2024.

2. ESTRATEGIA DE SEGURIDAD DIGITAL



3. SEGUIMIENTO A LA EJECUCIÓN DE LA ESTRATEGIA DE SEGURIDAD DIGITAL

ESTRATEGIA	AVANCES TERCER TRIMESTRE
Liderazgo de seguridad de la información	• Se inició la actualización de la política de seguridad de información evaluando los cambios que deben aplicarse para alinearse con el cumplimiento de la nueva versión de la norma ISO 27001:2022. • Se inició la definición del Manual de políticas de seguridad a cargo del Oficial de Seguridad de Información. * Avance del primer trimestre. 10% * Avance segundo trimestre: 0% * Avance tercer trimestre: 20% * Total de avance: 30%
Gestión de riesgos de seguridad de información	• Se llevó a cabo la actualización de activos de información, con corte al 30 de septiembre se encontraban pendientes por finalizar la gestión los procesos: Gestión Contractual Gestión de Atención a Establecimientos de Reclusión Gestión de Recursos Físicos y Suministros. • Se inició la actualización de riesgos de seguridad con el proceso Gestión de Tecnologías de la Información. * Avance del primer trimestre. 0% * Avance segundo trimestre: 10% * Avance del tercer trimestre: 40% * Total de avance: 50%
Concientización, sensibilización y capacitación	• Como parte de la implementación del plan de sensibilización, capacitación y socialización del SGSI se ejecutaron las siguientes actividades: ✔ Charlas de socialización de seguridad de información. ✔ Envío píldoras de seguridad (incluidas las de MinJusticia). ✔ Evidencias de evaluación de conocimientos básicos en seguridad de información * Avance del primer trimestre. 25% * Avance segundo trimestre: 25% * Avance tercer trimestre: 25% * Total de avance: 75%

Medición, revisión y evaluación del SGSI	• Se realiza seguimiento a los indicadores del SGSI dentro de los que se encuentran: Gestión de incidentes, gestión de riesgos y Actividades de sensibilización: o Registro total de 16 incidentes de seguridad, 100% de efectividad, no se reabrió ningún caso. Todos los casos fueron identificados como eventos de seguridad ya que no se impactó ningún activo de información. o Taller Actualización Gestión de Activos de Información o Se realizó un Test sobre Contraseñas Seguras previa a algunas píldoras enviadas, este test fue resuelto por 57 usuarios. o Taller de gestión de Riesgos de seguridad. • Se presentó en el Comité Institucional de Gestión y Desempeño el informe de revisión del SGSI del primer semestre 2024. * Avance del primer trimestre. 5% * Avance segundo trimestre: 45% * Avance tercer trimestre: 25% * Total de avance: 75%
Fortalecimiento de controles técnicos	• A través del Comité Institucional de Gestión y Desempeño se aprobó la actualización del procedimiento de control de cambios. • A través de la herramienta de Solarwinds se realizó el monitoreo de diferentes activos que componen la infraestructura tecnológica de la Entidad con el fin de analizar la capacidad, monitorear la disponibilidad de servicios y dispositivos configurados. Con el fin de formalizar esta gestión, se inició la actualización del procedimiento de gestión de la capacidad. • Se realizó la actualización del instructivo de borrado seguro. • A través del Contrato 162 de 2024 con la empresa Open Group SAS se ejecutaron las siguientes actividades: o Cambio e instalación de chasis de los firewall 601E a 400F o Migración de los dispositivos y arquitectura de seguridad perimetral Firewall. o Entrega de gestión del Firewall por parte del proveedor. o Transferencia de conocimiento de la plataforma de seguridad perimetral. o Instalación del agente FortiEDR en los servidores de la Entidad. o Pruebas de alta disponibilidad de firewalls. o Se llevó a cabo el KickOff sobre el EDR (Analizador de Comportamientos en la Red). o Con la fábrica de Fortinet, se ejecutaron 4 sesiones de Best Practices. o Se realizó por parte del proveedor OPenGroup entrega parcial del Instructivo y Matrices de Escalamientos del CDS (Centro de Servicio). o Por último se realizó en conjunto con el Proveedor OpenGroup validación de la Ficha Técnica contractual * Avance del primer trimestre. 5% * Avance segundo trimestre: 30% * Avance tercer trimestre: 40% * Total de avance: 75%

Transición de la Norma ISO 27001:2013 a la 27001:2022	• Se realiza la revisión y actualización del SOA, con el fin de evaluar los controles de la nueva versión de la norma ISO 27001:2022. * Avance del primer trimestre. 30% * Avance segundo trimestre: 0% * Avance tercer trimestre: 40% * Total de avance: 70%

4. CONCLUSIONES

Teniendo en cuenta la gestión realizada, durante el tercer trimestre se avanzó en un 32% del cumplimento de acuerdo con las actividades propuestas, y un porcentaje acumulado para la vigencia de 62% cumpliendo así con el porcentaje de avance programado en el plan de acción.

Las estrategias con las cuales se avanzó en el trimestre son:

- Liderazgo de la seguridad de información
- Gestión de riesgos de seguridad de información
- Concientización, Sensibilización y Capacitación
- Medición, revisión y evaluación del SGSI
- Fortalecimiento de controles técnicos
- Transición de la Norma ISO 27001:2013 a la 27001:2022

IMELDA MUÑOZ MANCIPE
JEFE OFICINA DE TECNOLOGÍA

Elaboró: Daniel Muñoz Oficial de Seguridad de la Información USPEC - Mayra Agudelo Profesional Especializado OTEC