UNIDAD DE SERVICIOS PENITENCIARIOS Y CARCELARIOS - USPEC

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

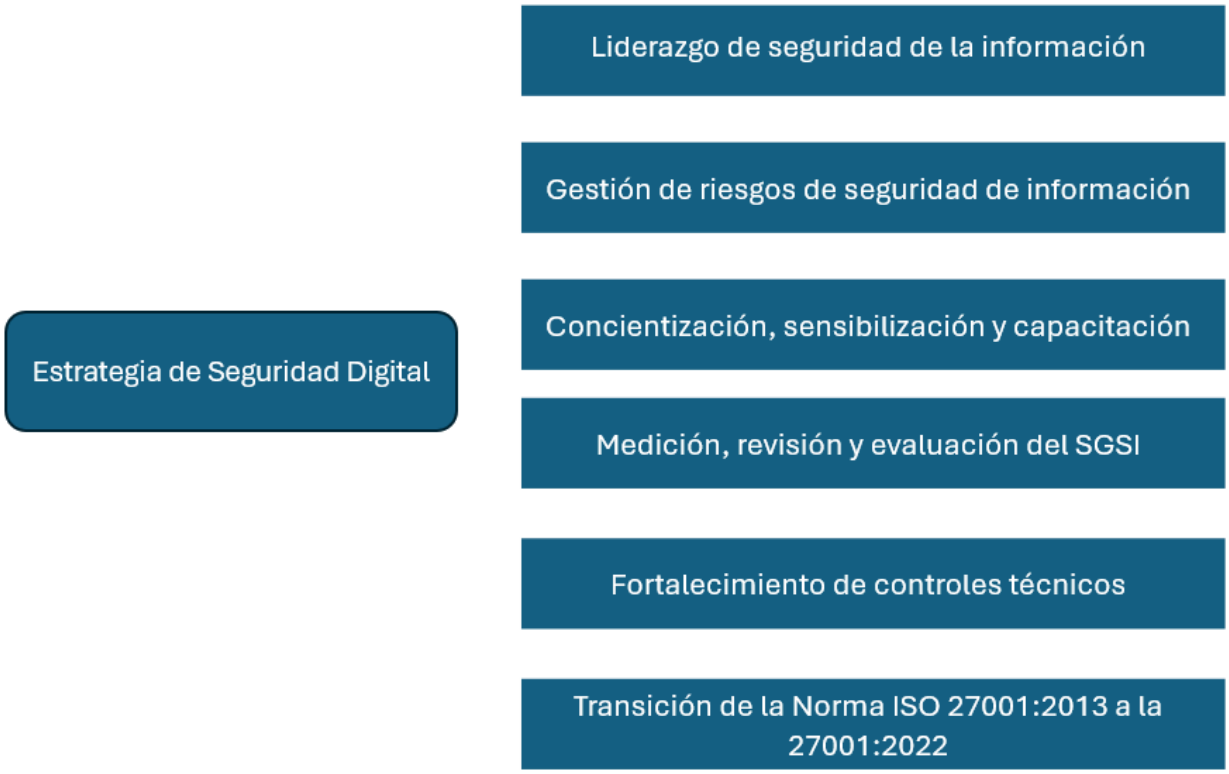
BOGOTÁ D.C., 27 DE DICIEMBRE 2024

CUARTO 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 CUARTO TRIMESTRE
Liderazgo de seguridad de la información	● Se actualizó la Política de Seguridad y Privacidad de Información y fue aprobada por parte del Comité Institucional de Gestión y Desempeño. Teniendo en cuenta que el documento se actualizó como resolución, con corte al 27 de diciembre se encontraba pendiente por cargar en el INFODOC con el fin de lograr la aprobación formal y posterior publicación en el portal web de la Entidad. ● Se elaboró y aprobó por parte del Comité Institucional de Gestión y Desempeño el Manual de políticas de seguridad a cargo del Oficial de Seguridad de Información. ● Se actualizó y aprobó la Guía de Borrado Seguro y el procedimiento de Gestión de la Capacidad por parte del Comité Institucional de Gestión y Desempeño. * Avance del primer trimestre. 10% * Avance segundo trimestre: 0% * Avance tercer trimestre: 20% * Avance del cuarto trimestre: 60% * Total de avance: 90%
Gestión de riesgos de seguridad de información	● Con corte al 27 de diciembre, se llevó a cabo la validación y ajuste de activos de información, con los delegados de los siguientes procesos: 1. Gestión Contractual 2. Gestión de Atención a Establecimientos de Reclusión 3. Gestión de Recursos Físicos y Suministros. 4. Gestión Tecnologías de la Información 5. Gestión Estratégica Organizacional 6. Gestión de Talento Humano 7. Gestión de la Comunicación Institucional 8. Gestión Financiera 9. Gestión de Suministro de Bienes y Prestación de Servicios 10. Gestión de Infraestructura 11. Gestión Jurídica Los demás procesos no confirmaron el estado de su inventario de activos. ● Se avanzó con la actualización de riesgos de seguridad y plan de tratamiento del proceso Gestión de Tecnologías de la Información. Adicionalmente se inició el análisis de riesgos con los demás procesos institucionales, logrando la identificación de riesgos de seguridad. Se tiene proyectado en el mes de enero dar continuidad a esta actividad con el fin de generar el mapa final de riesgos y el PTR para la vigencia 2025. * Avance del primer trimestre. 0% * Avance segundo trimestre: 10% * Avance del tercer trimestre: 40%

	* Avance del cuarto trimestre: 20% * Total de avance: 70%
Concientización, sensibilización y capacitación	• Como parte de la implementación del plan de sensibilización, capacitación y socialización del SGSI se ejecutaron las siguientes actividades: ✔ Sesiones de validación de Activos de Información y Riesgos de Seguridad de la Información con los delegados. ✔ Envío píldoras de seguridad (incluidas las de MinJusticia). * Avance del primer trimestre. 25% * Avance segundo trimestre: 25% * Avance tercer trimestre: 25% * Avance cuarto trimestre: 25% * Total de avance:100%
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: ○ Indicador de incidentes. Registro total de 43 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. ○ Gestión de riesgos. Durante el cuarto trimestre se avanzó en un 17% de las actividades propuestas, contando con un porcentaje acumulado del 90% ○ Se realizan envíos de píldoras de Seguridad y para el último trimestre no se realizan pruebas o test de seguridad de la información. • Se presentó en el Comité Institucional de Gestión y Desempeño el informe de revisión del SGSI del segundo semestre 2024. • Se contrató la firma Five Strategy (Cto. 285 de 2024) a través de la cual se ejecutará el proceso de ethical hacking, gestión de vulnerabilidades, pentesting, phishing y auditoría de seguridad. El 26 de diciembre se realizó la reunión de apertura de la auditoría con el fin de ejecutarla en el mes de enero, las demás actividades alcance del contrato se ejecutarán en los meses de enero a abril del 2025. * Avance del primer trimestre. 5% * Avance segundo trimestre: 45% * Avance tercer trimestre: 25% * Avance cuarto trimestre: 15% * Total de avance: 90%

Fortalecimiento de controles técnicos	● A través del Comité Institucional de Gestión y Desempeño se aprobó la actualización del procedimiento de gestión de la capacidad y la guía de borrado seguro. ● Se solicitó el avance del proceso de copias de seguridad, con el fin de tener respaldo de la información crítica de la Entidad, se realiza un proceso de copiado de la información de forma paralela en un disco duro externo para reducir el impacto de disponibilidad. ● 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. ● A través del Contrato 162 de 2024 con la empresa Open Group SAS se ejecutaron las siguientes actividades: ○ Ajuste de configuraciones canal de internet secundario, configuración de SD-WAN. ○ Se realiza el cambio de licenciamiento EDR disponible para servidores se ajustó para ser usado en clientes. ○ Se realiza activación de escudos de protección EDR en clientes remotos. ○ Gestión de casos para excepciones del agente EDR en clientes remotos. * Avance del primer trimestre. 5% * Avance segundo trimestre: 30% * Avance tercer trimestre: 40% * Avance cuarto trimestre: 25% * Total de avance: 100%
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. ● Se realiza la revisión de Riesgos de seguridad basado en los 93 controles de la nueva versión de la norma. ● Se gestiona y aprueba por el Manual de Seguridad de la Información el cual incluye los nuevos controles de la norma. * Avance del primer trimestre. 30% * Avance segundo trimestre: 0% * Avance tercer trimestre: 40% * Avance cuarto trimestre: 30% * Total de avance: 100%

4. CONCLUSIONES

Teniendo en cuenta la gestión realizada, durante el cuarto trimestre se avanzó en un 30% del cumplimento de acuerdo con las actividades propuestas, y un porcentaje acumulado para la vigencia de 92%.

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

Teniendo en cuenta los tiempos de contratación del proceso de Ethical Hacking y Auditoría de seguridad de información, no fue posible ejecutar el proceso de validación del SGSI durante la presente vigencia, sin embargo se dio inicio a la auditoría a través de la reunión de apertura realizada el 26 de diciembre. Se planeó ejecutar esta auditoría en el mes de enero 2025,

Se presentaron retrasos en la actualización del mapa de riesgos de seguridad y plan de tratamiento, con los procesos involucrados, debido a la inasistencia de la mayoría de procesos a las actividades de sensibilización frente al tema y al incumplimiento del cronograma propuesto por el Oficial de Seguridad de Información.

En cuanto a la actualización de la Política de Seguridad y Privacidad de Información, la aprobación formal (a través del software INFODOC) se encuentra en proceso, Con corte al 30 de diciembre se encontraba en control de legalidad a cargo de la Oficina Asesora Jurídica.

Por lo anterior no fue posible durante la vigencia alcanzar un porcentaje de implementación del Plan Estratégico de Seguridad del 100%.

IMELDA MUÑOZ MANCIPE
JEFE OFICINA DE TECNOLOGÍA

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