Sistema de Gestión de Seguridad de la Información (SGSI) – Transport for London.

Implementación del estándar ISO/IEC 27001 para fortalecer la resiliencia digital y la confianza pública en la red de transporte más compleja del mundo.

Proyecto: Proyecto Final de Ciberseguridad.

Fecha de Ejecución: Febrero 2026

Elaborado por: Jose Rodriguez

Introducción y Propósito

El SGSI tiene como objetivo establecer un marco de gestión que proteja los activos de información que habilitan la movilidad segura.

- **Misión**: Garantizar que la seguridad digital sea el soporte de la seguridad física.
- **Visión:** Alineación total con la iniciativa "Vision Zero": la integridad de los datos es fundamental para eliminar accidentes graves y muertes en la red para 2041.

Alcance del SGSI

El alcance se delimita a los Sistemas de Gestión de Datos de Seguridad y Protección de la Red.

- **Incluye:** Red de videovigilancia (CCTV), sistemas de reporte de crímenes, datos de soporte a víctimas (Sarah Hope Line) y registros de violencia laboral (WVA).
- **Excluye:** Sistemas administrativos de soporte que no impactan directamente en la operación de transporte o seguridad pública.

Metodología de Gestión de Riesgos

Proceso sistemático basado en la norma ISO/IEC 27005 para la identificación, análisis y evaluación de riesgos.

- **Enfoque:** Análisis de impacto operativo, legal y reputacional.
- **Objetivo:** Detectar amenazas (como ciberataques a la infraestructura) y vulnerabilidades (como protocolos de red desactualizados) antes de que afecten la continuidad del servicio.

Hallazgos de la Evaluación de Riesgos

Identificación de amenazas críticas tras el análisis técnico:

- **Crítico:** Fraude y denegación de servicio en sistemas de pago Oyster/Contactless.
- **Alto:** Manipulación o pérdida de integridad en la evidencia digital de CCTV.
- **Alto:** Filtración de datos sensibles de víctimas y familiares atendidos por la línea Sarah Hope.

Tratamiento de Riesgos y Controles Seleccionados

Aplicación de controles del Anexo A para mitigar los niveles de riesgo inaceptables:

- **Criptografía:** Cifrado de extremo a extremo para datos financieros y evidencia forense.
- **Seguridad Física:** Control de acceso biométrico y perímetros reforzados en centros de control de tráfico.
- **Gestión de Incidentes:** Protocolos de escalamiento y respuesta rápida coordinados con la British Transport Police.

Gobernanza y Estructura RACI

Definición de responsabilidades para asegurar la sostenibilidad del sistema:

- **Panel de Seguridad y Sostenibilidad:** Supervisión estratégica y asignación de recursos.
- **CISO:** Liderazgo en la ejecución técnica y cumplimiento normativo.
- **Custodios de Datos:** Equipos de WVA y administradores de CCTV responsables de la integridad y privacidad de los registros.

Operación y Mejora Continua

Gestión adaptativa mediante el ciclo PDCA (Plan-Do-Check-Act):

- **Capacitación:** Integración de la ciberseguridad en los programas de entrenamiento de "Body Worn Video" (BWV) y gestión de conflictos para el personal de campo.
- **Resiliencia:** Evolución constante frente a nuevas amenazas dirigidas a los sistemas de transporte inteligente.

Evaluación del Desempeño y Auditoría

Verificación de la eficacia del SGSI:

- **KPIs:** Monitoreo del tiempo de respuesta ante incidentes (MTTR) y efectividad del parcheo de vulnerabilidades.
- **Auditoría Interna:** Revisiones semestrales de logs de acceso y pruebas de cumplimiento físico en estaciones para garantizar la vigencia de la certificación.

Conclusiones y Recomendaciones

El SGSI no es solo un requisito técnico, sino un escudo que blinda la confianza del ciudadano en TfL.

- **Impacto:** Datos protegidos equivalen a una red de transporte más segura y transparente.
- **Recomendación:** Proceder con la implementación de los controles de alta prioridad y mantener la transparencia informativa como eje central de la gestión pública.