Informe de visión general del SGSI aplicado a TfL.

Proyecto: Desarrollo de un Sistema Básico de Gestión de Seguridad de la Información (SGSI) para una Organización Pública

Fecha de Ejecución: Febrero 2026

Elaborado por: Jose Rodriguez

ÍNDICE

1. Resumen Ejecutivo

Este informe presenta el plan para organizar y proteger la información de Transport for London (TfL). El propósito principal es asegurar que los datos de los pasajeros y del personal estén siempre bien cuidados, evitando que caigan en manos equivocadas o se pierdan.

El trabajo se enfoca en partes fundamentales del servicio, como el sistema para denunciar delitos, las cámaras de vigilancia, el apoyo a las personas afectadas por accidentes y el cobro de pasajes con tarjetas. Al analizar estas áreas, se descubrió que existen peligros, como posibles ataques informáticos o fallos en los equipos, que podrían poner en riesgo la confianza de los usuarios o interrumpir el transporte.

Para solucionar estos problemas, el proyecto propone medidas claras:

- Mejorar la seguridad física en las oficinas y estaciones donde se guarda la información.
- Enseñar a los trabajadores a proteger sus claves y datos mientras hacen su labor diaria.
- Crear reglas estrictas para decidir quién tiene permiso de ver información delicada.

Este esfuerzo ayuda directamente a la meta de la organización de eliminar accidentes graves en la red de transporte ("Vision Zero"). Al tener datos seguros y confiables, la dirección puede tomar mejores decisiones para proteger a las personas. Por último, el plan incluye revisiones periódicas para verificar que todo funcione correctamente y corregir cualquier fallo de manera rápida, manteniendo el sistema actualizado frente a nuevas amenazas.

2. Alcance del SGSI

Naturaleza de la Organización

Transport for London (TfL) se constituye como la autoridad estatutaria responsable de la gestión integral del sistema de transporte en el Gran Londres. Su infraestructura abarca una red multimodal de alta complejidad que incluye el Metro de Londres (London Underground), servicios de autobuses, ferrocarriles y la red de carreteras principales.

La entidad opera como un nexo crítico para la movilidad urbana, gestionando sistemas tecnológicos a gran escala que soportan la operación diaria de millones de trayectos y la coordinación con autoridades policiales para garantizar la seguridad en la red.

Objetivos Estratégicos e Iniciativas Clave

La estrategia organizacional está fundamentada en el compromiso "Vision Zero", una iniciativa de seguridad vial y operativa cuyo objetivo es la eliminación total de muertes y lesiones graves en la red de transporte para el año 2041.

Este objetivo estratégico exige una infraestructura resiliente que permita el análisis de datos para la prevención de peligros y la gestión proactiva de riesgos operativos. La seguridad de la información se vuelve un habilitador crítico para asegurar la integridad de los sistemas que monitorizan y protegen la vida de los usuarios.

Procesos Críticos y Gestión de Activos de Información

La operatividad de TfL depende de la gestión técnica de diversos activos de información, articulados a través de procesos críticos de reporte, vigilancia y soporte:

- **Gestión de Reportes de Incidentes y Seguridad Pública:** TfL administra flujos de datos provenientes de herramientas de reporte en línea y telefónicas para la captación de crímenes, riesgos de seguridad y conductas antisociales. Estos registros constituyen activos de información esenciales para la respuesta operativa y la colaboración con la British Transport Police.
- **Vigilancia y Evidencia Digital (CCTV):** La red de videovigilancia genera activos de información de alta sensibilidad. Las imágenes capturadas son fundamentales para procesos de investigación forense, aunque están sujetas a políticas estrictas de retención temporal y privacidad de datos.
- **Protección del Personal y Base de Datos de Agresiones:** El sistema de registro de Violencia y Agresión Relacionada con el Trabajo (WVA) centraliza datos sobre incidentes contra empleados. Este activo permite el análisis de patrones para el despliegue de oficiales de refuerzo (TSE Officers) y la implementación de dispositivos Body Worn Video (BWV).
- **Sistemas de Soporte y Datos de Víctimas:** La gestión de información a través de la línea Sarah Hope y servicios de apoyo tras incidentes graves involucra el manejo de datos personales y médicos altamente sensibles. La confidencialidad de estos activos es imperativa para cumplir con el compromiso de apertura y apoyo institucional.
- **Gestión de Cuentas y Datos Transaccionales:** Los sistemas asociados a tarjetas Oyster y pagos sin contacto (contactless) representan activos de información críticos bajo estándares de seguridad financiera, cuya protección es vital para prevenir el fraude y garantizar la privacidad de los trayectos de los ciudadanos.

Este inventario técnico de activos y procesos subraya la necesidad de un marco de control bajo la norma ISO 27001 para mitigar las amenazas que podrían comprometer la continuidad del transporte londinense y la seguridad de sus datos.

3. Resultados de la Evaluación de Riesgos

Metodología de Evaluación

Se ha empleado un enfoque basado en activos. Para cada sistema, se identificaron los activos de información primarios, las amenazas que podrían explotar vulnerabilidades existentes y el impacto resultante en la operación de TfL. El nivel de riesgo se determina mediante la combinación cualitativa de la probabilidad de ocurrencia y el impacto institucional (legal, financiero y reputacional).

Análisis por Sistema

- **Gestión de Reportes de Incidentes y Seguridad Pública:** Este sistema procesa datos operativos sobre delitos y conductas antisociales. El riesgo principal reside en el acceso no autorizado a bases de datos de reportes activos, lo que podría comprometer investigaciones en curso con la British Transport Police. La integridad de estos reportes es crítica para el análisis estadístico que sustenta la iniciativa "Vision Zero".
- **Vigilancia y Evidencia Digital (CCTV):** Los activos de video son fundamentales para la seguridad física y la procuración de justicia. El análisis identifica riesgos de fuga de información (confidencialidad) y manipulación de evidencia (integridad). Las vulnerabilidades técnicas en los nodos de almacenamiento y la falta de cifrado en segmentos de red antiguos representan vectores de ataque significativos.
- **Sistemas de Soporte y Datos de Víctimas (Sarah Hope Line):** Este sistema gestiona Datos de Carácter Personal de Categoría Especial (salud y antecedentes de incidentes graves). Dado el compromiso de TfL con la transparencia y el apoyo compasivo, una brecha en la confidencialidad tendría un impacto crítico en la reputación y conllevaría sanciones legales severas bajo el GDPR. El riesgo de ingeniería social hacia los operadores es elevado.
- **Gestión de Cuentas y Datos Transaccionales (Oyster/Contactless):** La infraestructura financiera de pagos es un objetivo primario para el fraude cibernético. Se analizan riesgos de interceptación de datos de pago y alteración de saldos. La disponibilidad del sistema de validación es esencial para evitar el colapso operativo en horas punta en estaciones de alta concurrencia.

Tabla de Evaluación de Riesgos (ISO 27001)

Calificación de Riesgo	Descripcion
Prioridad Crítica	Se requiere la implementación inmediata de cifrado de extremo a extremo en la red transaccional y revisión de la seguridad física de los lectores de tarjetas.
Prioridad Alta	Es imperativo robustecer la seguridad de la capa de aplicación en los portales web y migrar la infraestructura de CCTV a una red privada virtualizada con protocolos de transporte seguro (SRTP).
Prioridad Media	Se debe proceder con la actualización de las políticas de control de acceso y la mejora de la seguridad física en los gabinetes técnicos de las estaciones.

4. Lista de Controles Seleccionados / Declaración de Aplicabilidad

Seguridad Física y Ambiental (Dominio A.7)

Dada la naturaleza crítica de la infraestructura de transporte de Londres, la protección de los activos físicos es imperativa para garantizar la continuidad del servicio y la integridad de los datos.

- **Protección de Centros de Control:** Los centros de control de tráfico y de gestión de red (como los del Metro de Londres) se clasifican como áreas seguras. Se requiere la implementación del control A.7.2 (Entrada física) para restringir el acceso únicamente a personal autorizado mediante autenticación biométrica o tarjetas inteligentes, protegiendo los terminales que gestionan la red ferroviaria y de carreteras.
- **Aseguramiento de la Vigilancia (CCTV):** Las cámaras de CCTV son activos duales: actúan como medida de seguridad física y como generadores de evidencia digital. Bajo el control A.7.12 (Seguridad del cableado y equipos), es necesario proteger físicamente los nodos de comunicación y dispositivos de grabación situados en estaciones para prevenir el sabotaje o la extracción no autorizada de discos duros que contienen evidencia forense.

Gestión de Incidentes de Seguridad de la Información (Dominio A.5)

TfL ya cuenta con mecanismos robustos para el reporte de crímenes e incidentes operativos. El SGSI debe integrar la respuesta ante brechas de datos en este ecosistema existente.

- **Procedimientos de Escalamiento:** En cumplimiento con el control A.5.24 (Gestión de incidentes de seguridad de la información), se deben establecer canales claros para que el personal de atención al cliente y los oficiales de apoyo (TSE) escalen anomalías digitales, como el compromiso de datos de la línea Sarah Hope o la interceptación de transacciones Oyster.
- **Respuesta y Recolección de Evidencia:** Ante un incidente de transporte grave, el control A.5.28 (Recolección de evidencia) asegura que el material de CCTV y los logs de acceso a los sistemas de seguridad se preserven adecuadamente para su posterior análisis forense y cumplimiento con el "Compromiso de Apertura" de la organización.

Concienciación y Formación en Seguridad (Dominio A.6)

El factor humano es un vector de riesgo crítico, especialmente en roles de cara al público que manejan dispositivos móviles y acceso a bases de datos policiales.

- **Integración en Capacitaciones Existentes:** TfL imparte de forma obligatoria programas de gestión de conflictos y de-escalación para su personal. Bajo el control A.6.3 (Concienciación, educación y formación), se debe anexar un módulo de higiene digital. Esto incluye el manejo seguro de dispositivos de video corporal (Body Worn Video - BWV) y la protección de credenciales al realizar consultas en el Police National Computer (PNC).
- **Cultura de Seguridad:** La formación debe enfocarse en que el personal reconozca que la protección de la información de los pasajeros (ej. rutas de viaje o datos de víctimas) es una extensión directa de su responsabilidad primordial de garantizar la seguridad física en la red.

5. Políticas y Procedimientos de Seguridad

Marco de Políticas: Transparencia y Control de Acceso

El desarrollo de las políticas de seguridad en TfL no solo responde al cumplimiento de la norma ISO 27001, sino que se integra con el "Compromiso con la Apertura" (Commitment to Openness) de la organización. Este compromiso exige que la seguridad de la información actúe como un facilitador de la transparencia, especialmente en la gestión de datos tras incidentes graves o muertes en la red.

- **Política de Seguridad de la Información:** Debe reflejar que la protección de los datos es fundamental para mantener la honestidad con el público y los familiares de las víctimas. La transparencia se garantiza mediante la integridad de los datos; solo una información veraz y protegida puede ser comunicada de manera abierta y sensible.
- **Política de Control de Acceso:** Se enfoca en la gestión de identidades para sistemas críticos como el reporte de crímenes y el acceso a evidencia de CCTV. Se debe implementar un modelo de Control de Acceso Basado en Roles (RBAC) que asegure que el acceso a datos sensibles (como los de la línea Sarah Hope o registros de agresiones al personal) esté estrictamente limitado a personal autorizado, garantizando que la apertura institucional no comprometa la privacidad de los individuos.

Manual del SGSI y Estructura de Gobernanza

El Manual del SGSI se constituye como el documento maestro que articula la estrategia de seguridad con la estructura operativa de TfL. La gobernanza de la seguridad de la información se integra en los niveles de decisión más altos de la entidad para asegurar la resiliencia del transporte londinense.

- **Integración con Paneles Directivos**: El manual describe la participación activa del panel de "Safety, Sustainability & HR", el cual ya supervisa trimestralmente el trabajo para eliminar la violencia laboral (WVA). Bajo el SGSI, este panel adquiere responsabilidades de supervisión sobre la eficacia de los controles de seguridad de la información, asegurando que la protección de los empleados y los activos digitales esté alineada con los objetivos de sostenibilidad y seguridad física.
- **Gestión de Responsabilidades:** El documento detalla los roles técnicos y administrativos, desde los oficiales de cumplimiento hasta los técnicos de campo que operan con sistemas como el Police National Computer (PNC) o dispositivos de video corporal (BWV). El manual establece que la seguridad de la información es una responsabilidad compartida que soporta directamente el objetivo "Vision Zero", protegiendo los datos que permiten prevenir muertes y lesiones graves en la red de transporte.
- **Mejora Continua y Auditoría:** El manual define los procesos de revisión por la dirección y auditoría interna, utilizando la información de los informes de seguridad y salud para identificar áreas de mejora en el tratamiento de los riesgos de información.

7. Conclusiones y Recomendaciones

Marco de Revisión Continua (Alineación con Guía 03 y Vision Zero)

La implementación del SGSI en TfL no se considera un estado estático, sino un componente dinámico que apoya directamente la iniciativa estratégica "Vision Zero", cuyo fin es eliminar todas las muertes y lesiones graves en la red para 2041. La consecución de este objetivo depende de la disponibilidad e integridad de los datos de seguridad vial y análisis de riesgos. Siguiendo las directrices de la Guía 03, TfL debe establecer un proceso de revisión que garantice que los sistemas digitales que gestionan la seguridad operativa (como los avisos de peligro en carretera y los informes de colisiones) permanezcan resilientes y libres de manipulación.

Acción: Auditorías Trimestrales de Logs en Sistemas de Reporte
La planificación de auditorías internas trimestrales enfocadas en los logs de acceso de los sistemas de reporte de crímenes es una medida de control crítico para la confianza pública.

- **Protección de Datos en el Transporte:** TfL gestiona información altamente sensible, incluyendo denuncias de ofensas sexuales, crímenes de odio y datos de víctimas a través de la línea Sarah Hope.
- **Justificación Técnica:** La revisión sistemática de los registros de auditoría permite verificar la trazabilidad de los accesos, asegurando que solo el personal autorizado (como los oficiales de Transport Support and Enforcement - TSE) consulte información sensible. Esto previene brechas de confidencialidad que podrían disuadir a los usuarios de reportar incidentes, comprometiendo así los datos necesarios para que TfL ejecute sus estrategias de prevención del delito y seguridad ciudadana.

Resolución de No Conformidades y Mejora de la Fase 2
La auditoría externa de Fase 2 representa la validación in situ de que los controles de seguridad están efectivamente protegiendo la red de transporte.

- **Gestión de Hallazgos:** La definición de un protocolo para corregir no conformidades es vital para la resiliencia del transporte público. Si se detectara, por ejemplo, una debilidad en la retención de evidencia de CCTV o en la protección de las cuentas Oyster/contactless, TfL debe aplicar análisis de causa raíz para remediar la vulnerabilidad antes de que sea explotada.
- **Impacto Operativo:** Al resolver estas deficiencias, el SGSI actúa como un escudo para los sistemas tecnológicos que habilitan el transporte seguro. La corrección inmediata de fallos en el manejo de datos de seguridad garantiza que la toma de decisiones basada en datos (pilar de "Vision Zero") se realice sobre información fidedigna, protegiendo tanto la integridad física de los pasajeros como su privacidad digital.