Manual del SGSI: Transport for London (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 resumen presenta el contenido del Manual del SGSI para Transport for London (TfL), un documento que sirve como guía para organizar y proteger la información importante de la institución.

El objetivo principal es asegurar que los datos que maneja TfL (como los viajes de los pasajeros, los reportes de incidentes y la información del personal) se mantengan seguros, privados y siempre disponibles cuando se necesiten.

Puntos clave del manual:

- **Protección integral:** El plan no solo busca proteger computadoras, sino que vincula la seguridad digital con la seguridad física de las personas. Esto apoya directamente la meta de la organización de eliminar accidentes graves en el transporte ("Vision Zero").
- **Responsables claros:** Se definen quiénes son los encargados de vigilar la seguridad, desde los directivos que toman las decisiones hasta el personal técnico que cuida las cámaras de vigilancia y los sistemas de pago con tarjeta.
- **Gestión de riesgos:** El manual explica cómo identificar posibles peligros (como robos de datos o fallos en los sistemas) y qué medidas tomar para evitar que ocurran o para reducir su impacto.
- **Capacitación del personal:** Se destaca la importancia de que todos los trabajadores sepan cómo manejar la información de forma segura, integrando estos consejos en sus entrenamientos diarios de servicio al cliente.
- **Revisiones y mejoras:** El sistema no es fijo; se revisa constantemente mediante auditorías para encontrar fallos y corregirlos rápido. Esto permite que TfL se mantenga al día frente a nuevos tipos de ataques o problemas tecnológicos.
- **Cuidado de los archivos:** Se establecen reglas sobre cuánto tiempo se deben guardar las imágenes de las cámaras y los reportes de accidentes, respetando siempre las leyes de protección de datos y el compromiso de la empresa de ser transparente con el público.

En conclusión, este manual es la herramienta que permite a TfL funcionar de manera confiable, protegiendo tanto la tecnología que hace mover a la ciudad como la privacidad de quienes viven en ella.

1. Introducción y Propósito

Introducción y Propósito

El presente Manual del Sistema de Gestión de Seguridad de la Información (SGSI) constituye el pilar documental estratégico para la gobernanza de la ciberseguridad dentro de Transport for London (TfL). En un entorno de transporte multimodal de alta complejidad, la protección de la información no se limita a la salvaguarda de datos digitales, sino que se integra como un componente esencial de la seguridad operativa y la confianza pública.

Objetivo del Manual

El objetivo primordial de este documento es definir y formalizar el marco de gestión técnica y administrativa necesario para proteger los activos de información críticos de TfL. Esto implica garantizar la Confidencialidad, Integridad y Disponibilidad de sistemas vitales, tales como la infraestructura de videovigilancia (CCTV), los registros de incidentes de seguridad ciudadana, los datos transaccionales de medios de pago (Oyster y Contactless) y la información de soporte a víctimas de incidentes graves. El manual establece las directrices para identificar riesgos, implementar controles proporcionales y asegurar la resiliencia operativa ante amenazas emergentes en el ecosistema del transporte urbano.

Misión y Visión de Seguridad: Alineación con "Vision Zero"

La visión de seguridad de la información en TfL trasciende el ámbito técnico para alinearse directamente con la iniciativa estratégica "Vision Zero", cuyo mandato es la eliminación total de muertes y lesiones graves en la red de transporte para el año 2041.

Bajo este paradigma, la seguridad se aborda de forma holística: la seguridad física y la seguridad digital actúan como un todo indivisible. Un sistema de información íntegro y disponible es el que permite el análisis de datos preventivos, la respuesta inmediata de los servicios de emergencia y la transparencia en la comunicación tras incidentes críticos. Por tanto, la misión del SGSI es blindar los procesos digitales que habilitan un transporte físico seguro, asegurando que la toma de decisiones basada en datos se realice sobre información fidedigna y protegida.

Audiencia

Este manual es de aplicación obligatoria y ha sido redactado para una audiencia técnica y administrativa diversa, que garantiza la operatividad de la red:

- **Personal Administrativo y Operativo:** Empleados directos de TfL, incluyendo los oficiales de Transport Support and Enforcement (TSE), quienes gestionan datos de cumplimiento y seguridad en campo.
- **Contratistas y Proveedores de Servicios:** Entidades externas que administran infraestructuras tecnológicas, mantenimiento de sistemas de recaudo o servicios de soporte técnico.
- **Socios Estratégicos:** Organismos de seguridad pública, principalmente la British Transport Police (BTP) y la Policía Metropolitana, así como servicios de emergencia, quienes dependen de la disponibilidad y el intercambio seguro de información para la protección de la red y sus usuarios.

2. Contexto de la Organización

Comprensión de TfL

Transport for London (TfL) opera como la autoridad estatutaria responsable de la implementación de la estrategia de transporte y la gestión de los servicios de movilidad en el Gran Londres. Su infraestructura comprende una red multimodal integrada que incluye el Metro de Londres (London Underground), la red de autobuses, el Docklands Light Railway (DLR), servicios ferroviarios y la gestión de las principales arterias viales.

La operatividad de esta red presenta una dependencia tecnológica crítica. TfL gestiona sistemas de control de tráfico en tiempo real, infraestructuras de videovigilancia distribuida (CCTV) y plataformas digitales de recaudo y atención al cliente. Estos sistemas no solo facilitan el tránsito de millones de usuarios diarios, sino que son el soporte fundamental para la coordinación de respuestas ante emergencias y la recolección de datos operativos necesarios para alcanzar el objetivo estratégico "Vision Zero". La interrupción o el compromiso de estas tecnologías supondría un impacto severo en la seguridad física de la red y en la continuidad de los servicios esenciales de la ciudad.

Partes Interesadas

El ecosistema de seguridad de la información de TfL involucra a diversas partes interesadas, cuyas necesidades y expectativas definen los requisitos del SGSI:

- **Pasajeros:** Requieren la garantía de confidencialidad y protección de su privacidad, especialmente en lo relativo a los datos de geolocalización de trayectos y la seguridad de la información financiera asociada a las cuentas Oyster y pagos contactless.
- **Empleados**: Especialmente el personal de cara al público y los oficiales de Transport Support and Enforcement (TSE). Su interés radica en la integridad de los sistemas de reporte de violencia laboral (WVA) y el manejo seguro de las grabaciones de dispositivos de video corporal (Body Worn Video), fundamentales para su protección frente a agresiones.
- **Organismos Reguladores:** Entidades que exigen el cumplimiento normativo en materia de protección de datos (como el GDPR) y estándares de seguridad para infraestructuras críticas de transporte.
- **Policía (British Transport Police y Policía Metropolitana):** Dependen de la disponibilidad y veracidad de la evidencia digital y los reportes de incidentes para la prevención del delito y la ejecución de investigaciones forenses en la red.

Alcance del SGSI

El alcance de este Sistema de Gestión de Seguridad de la Información se define de manera específica para cubrir los Sistemas de Gestión de Datos de Seguridad y Protección de la Red.

Este límite abarca los activos, procesos y personal involucrados en:

- La captación y tratamiento de reportes de crímenes e incidentes de seguridad ciudadana.
- La gestión y almacenamiento de evidencia digital proveniente de la red de CCTV.
- Los sistemas de soporte a víctimas y gestión de datos sensibles manejados por servicios como la línea Sarah Hope.
- La infraestructura de datos que soporta la estrategia de reducción de riesgos laborales y seguridad vial.

3. Liderazgo y Compromiso

La eficacia del Sistema de Gestión de Seguridad de la Información (SGSI) en Transport for London (TfL) depende de un liderazgo sólido que integre la ciberseguridad en la cultura operativa de la organización. La dirección de TfL asume la responsabilidad de alinear los objetivos de seguridad de la información con la protección física de los ciudadanos y la integridad de la infraestructura de transporte de Londres.

Política de Seguridad de la Información

La Política de Seguridad de la Información representa la declaración de alto nivel emitida y firmada por la alta dirección de TfL. Este documento establece el compromiso institucional para proteger los activos de información contra amenazas internas y externas, asegurando la continuidad de los servicios de transporte.

La política se fundamenta en la premisa de que la seguridad digital es un habilitador crítico para alcanzar la iniciativa "Vision Zero"; por tanto, la integridad de los datos de tráfico, la disponibilidad de los sistemas de reporte y la confidencialidad de la información de los usuarios son prioridades estratégicas. Asimismo, esta política refuerza el "Compromiso de Apertura", garantizando que la información sea gestionada de forma transparente y ética, especialmente en situaciones que involucren incidentes graves en la red.

Roles y Responsabilidades (Matriz RACI)

Para garantizar una ejecución coordinada, se establece una estructura de gobernanza donde las responsabilidades están claramente delimitadas mediante una matriz de asignación de responsabilidades (RACI):

- **Panel de Seguridad, Sostenibilidad y RR.HH. (Supervisión Estratégica):** Este organismo colegiado es el responsable último de la gobernanza del SGSI. Su función es supervisar de manera estratégica el cumplimiento de los objetivos de seguridad, revisar los informes de desempeño trimestrales y asegurar la asignación de recursos necesarios para mitigar riesgos críticos que afecten a la red.
- **Responsable de Seguridad de la Información - CISO (Ejecución Técnica):** Encargado de liderar la implementación operativa del SGSI. El CISO coordina la evaluación de riesgos, la selección de controles técnicos y la respuesta ante incidentes de ciberseguridad, asegurando que la arquitectura tecnológica de TfL cumpla con los estándares de la norma ISO 27001.
- **Equipo de WVA - Violencia y Agresión Relacionada con el Trabajo (Custodios de Datos):** Este equipo especializado actúa como custodio de los activos de información relativos a incidentes de seguridad del personal. Son responsables de garantizar la integridad y confidencialidad de los reportes de agresiones y los datos recolectados para la protección de los trabajadores de primera línea.
- **Administradores de CCTV (Responsables de Integridad):** Personal técnico encargado de la gestión de la red de videovigilancia. Su responsabilidad principal es asegurar la integridad de las grabaciones y el cumplimiento de las políticas de retención, garantizando que el material esté disponible para las autoridades policiales cuando sea requerido como evidencia digital.

4. Planificación y Gestión de Riesgos

La gestión de riesgos en Transport for London (TfL) constituye un proceso dinámico y transversal, diseñado para garantizar la resiliencia de la infraestructura de transporte y la protección de los datos de millones de ciudadanos. Este marco asegura que las decisiones de seguridad estén fundamentadas en el análisis técnico y alineadas con la seguridad operativa de la red.

Metodología de Evaluación de Riesgos

TfL adopta una metodología sistemática basada en el estándar internacional ISO/IEC 27005, la cual se integra en el ciclo de mejora continua del SGSI. Este proceso se divide en tres fases fundamentales:

- **Identificación:** Se realiza un inventario exhaustivo de los activos de información críticos, tales como la infraestructura de red de CCTV, los sistemas de recaudo Oyster/contactless y las bases de datos de soporte a víctimas (línea Sarah Hope). Se identifican las amenazas (ej. ataques de denegación de servicio o accesos no autorizados) y las vulnerabilidades asociadas a los protocolos de comunicación y al hardware situado en estaciones.
- **Análisis:** Se evalúa el nivel de riesgo mediante la combinación del impacto potencial (operativo, legal y reputacional) y la probabilidad de ocurrencia de la amenaza. Este análisis considera la efectividad de los controles ya existentes en la red ferroviaria y de autobuses.
- **Evaluación:** Los riesgos identificados se comparan con los umbrales de seguridad establecidos por la organización, permitiendo priorizar el tratamiento de aquellos que podrían afectar la disponibilidad del transporte público o la privacidad de los usuarios.

Criterios de Aceptación del Riesgo

Como autoridad de transporte y operador de infraestructuras críticas, TfL mantiene una postura de baja tolerancia al riesgo. Los criterios para definir qué niveles de riesgo son aceptables se fundamentan en la seguridad del servicio público:

- **Riesgos Críticos/Altos:** No se aceptan riesgos que comprometan la integridad física de los pasajeros, la disponibilidad de los sistemas de respuesta ante emergencias o la confidencialidad de datos sensibles de víctimas de incidentes graves. Estos riesgos requieren tratamiento inmediato a través de la implementación de controles técnicos robustos.
- **Riesgos Medios/Bajos:** Solo se consideran aceptables aquellos riesgos residuales cuyo impacto sea mínimo y cuya mitigación resulte desproporcionadamente costosa en relación con el beneficio obtenido. Estos riesgos permanecen bajo monitoreo constante para asegurar que no evolucionen hacia niveles inaceptables.

Plan de Tratamiento de Riesgos

Para los riesgos que superan el nivel de aceptación, TfL aplica un Plan de Tratamiento de Riesgos que utiliza los controles del Anexo A de la norma ISO 27001, adaptados específicamente al entorno de transporte londinense:

- **Mitigación técnica:** Aplicación de controles de criptografía para proteger los datos transaccionales y la evidencia digital generada por las cámaras corporales (Body Worn Video) y fijas.
- **Resiliencia física:** Implementación de medidas de seguridad ambiental y física en centros de control de tráfico y nodos de telecomunicaciones para prevenir sabotajes o interrupciones accidentales.
- **Gobernanza de incidentes:** Establecimiento de procedimientos de respuesta que se integran con los protocolos policiales existentes, asegurando que cualquier brecha de datos sea contenida y reportada de forma transparente, en cumplimiento con el "Compromiso de Apertura" de la organización.
- Soporte a la visión estratégica: El tratamiento de riesgos asegura que la infraestructura digital sea un soporte fiable para la iniciativa "Vision Zero", permitiendo que la toma de decisiones basada en datos para prevenir accidentes se realice sobre una base tecnológica segura y fidedigna.

5. Soporte y Recursos

Para asegurar la eficacia operativa del SGSI en Transport for London (TfL), la organización debe proveer los recursos necesarios que garanticen la resiliencia de la red. Este apartado detalla la gestión del talento, la formación técnica y los flujos de comunicación indispensables para proteger la infraestructura crítica de transporte.

Recursos Humanos: Competencias necesarias

La complejidad del ecosistema tecnológico de TfL exige que el personal técnico y administrativo posea competencias específicas alineadas con la seguridad operativa y la protección de datos:

- **Especialización técnica:** El personal encargado de la infraestructura debe poseer conocimientos avanzados en seguridad de redes multimodales, criptografía aplicada a sistemas de pago (Oyster/contactless) y gestión de activos de videovigilancia distribuida.
- **Marcos Normativos:** Es imperativo que los analistas de ciberseguridad dominen la norma ISO 27001 y las regulaciones locales de protección de datos (GDPR), dada la alta sensibilidad de los registros médicos y personales gestionados por servicios como la línea Sarah Hope.
- **Capacidad de Respuesta:** El personal de campo, incluidos los oficiales de Transport Support and Enforcement (TSE), debe estar capacitado en la identificación de anomalías digitales y físicas que puedan comprometer la seguridad de la red.

Concienciación y Capacitación: Integración de la Seguridad

TfL aprovecha sus programas formativos existentes para integrar la cultura de seguridad de la información, evitando silos de conocimiento y optimizando el tiempo de respuesta del personal:

- **Capacitación en Gestión de Conflictos:** Dado que TfL ya implementa programas obligatorios de gestión de conflictos y de-escalación para equipos operativos, se incorpora un módulo de higiene digital. Este enfoque asegura que el personal comprenda que proteger la información del pasajero es parte fundamental de su seguridad física.
- **Uso Seguro de Body Worn Video (BWV):** La formación específica para el uso de cámaras corporales incluye protocolos estrictos sobre la descarga, almacenamiento y cadena de custodia de las grabaciones. Esto garantiza que la evidencia digital recolectada para proteger al personal sea procesada de acuerdo con los estándares de integridad del SGSI.

Comunicación: Canales para el Reporte de Brechas

La comunicación es el eje que permite la detección temprana y la contención de incidentes. TfL establece canales robustos tanto internos como externos:

- **Canales Internos:** El personal operativo utiliza sistemas de reporte directo (como el equipo de WVA) para notificar incidentes de seguridad que afecten a los trabajadores o a los sistemas de control. Existen protocolos de escalonamiento hacia el CISO para brechas de datos identificadas en estaciones o centros de control.
- **Canales Externos:** En cumplimiento con el "Compromiso de Apertura", TfL mantiene líneas de comunicación transparentes con los pasajeros y familiares afectados por incidentes graves. Se establecen protocolos de comunicación segura con socios estratégicos como la British Transport Police para el intercambio de evidencia digital y reportes de crímenes en tiempo real.
- **Transparencia Institucional:** La organización utiliza su portal de seguridad y salud para emitir boletines trimestrales sobre el estado de la red, asegurando que la información sobre la efectividad de las medidas de seguridad sea accesible para las partes interesadas, reforzando la confianza en el sistema de transporte público.

6. Operación del SGSI

La fase de operación en Transport for London (TfL) representa la ejecución táctica de las estrategias de seguridad diseñadas para proteger la continuidad de la red de transporte. Esta sección detalla cómo se gestionan los cambios tecnológicos y se despliegan los controles técnicos en un entorno de alta disponibilidad y criticidad sistémica.

Planificación Operativa: Control de cambios en la infraestructura

Dada la magnitud de la red multimodal de TfL (Metro, Autobuses, DLR y Carreteras), cualquier modificación en la infraestructura tecnológica posee el potencial de generar riesgos operativos o brechas de seguridad.

- **Gestión de Cambios (Change Management):** Se establece un proceso riguroso de control de cambios para todas las actualizaciones en sistemas críticos, como la señalización ferroviaria o los nodos de comunicaciones de red. Este proceso exige una evaluación de impacto de seguridad previa a la implementación, asegurando que las actualizaciones no comprometan la integridad de la red.
- **Mantenimiento de la Disponibilidad:** La planificación operativa garantiza que las ventanas de mantenimiento no interfieran con la captación de datos de seguridad en tiempo real ni con la capacidad de respuesta de los servicios de emergencia, manteniendo la resiliencia necesaria para soportar la iniciativa "Vision Zero".

Implementación de Controles Críticos

La operación del SGSI prioriza la protección de activos de información que impactan directamente en la confianza del ciudadano y la seguridad física de los usuarios.

- **Control de Acceso a Sistemas de Reporte de Crímenes:**
    - Se implementan controles de autenticación robustos para los sistemas de reporte de incidentes y conductas antisociales.
    - El acceso a los datos de víctimas y reportes policiales está regido por el principio de "mínimo privilegio", asegurando que solo el personal autorizado de TfL y socios estratégicos como la British Transport Police (BTP) puedan consultar información sensible. Esto protege la confidencialidad de los ciudadanos que denuncian delitos de odio o acoso sexual en la red.
- **Cifrado de Datos de Tarjetas de Pago (Oyster/Contactless):**
    - Los datos transaccionales generados por millones de viajes diarios se consideran activos de alta sensibilidad financiera.
    - Se aplican protocolos de cifrado de extremo a extremo (E2EE) y estándares alineados con PCI-DSS para proteger la información de las cuentas Oyster y pagos contactless. El cifrado asegura que, en caso de interceptación de tráfico en los lectores de las estaciones, la información financiera de los usuarios permanezca ilegible y segura.
- **Seguridad Física en Centros de Control de Tráfico:**
    - Los centros de control, desde donde se monitoriza la seguridad de la red y el cumplimiento de "Vision Zero", se designan como zonas de alta seguridad.
    - Se despliegan perímetros de seguridad física, sistemas de detección de intrusiones y control de acceso biométrico para evitar el sabotaje o acceso no autorizado a las consolas de mando que gestionan el tráfico de Londres. La seguridad física de estos centros garantiza la integridad de los sistemas de videovigilancia (CCTV) y la continuidad de las comunicaciones críticas de la red.

7. Evaluación del Desempeño

La evaluación del desempeño en Transport for London (TfL) asegura que el SGSI no solo cumpla con los requisitos normativos de la ISO 27001, sino que sea una herramienta eficaz para proteger la infraestructura crítica y la privacidad de los millones de ciudadanos que utilizan la red. Este proceso de supervisión es fundamental para mantener la integridad de los datos que soportan la iniciativa estratégica "Vision Zero".

Seguimiento, Medición y Análisis

TfL establece mecanismos técnicos para medir de forma objetiva la eficacia de los controles implementados. Los indicadores clave de desempeño (KPIs) de seguridad de la información se definen para reflejar la salud de los activos críticos:

- **Tiempo de Respuesta ante Incidentes (MTTR):** Medición del tiempo transcurrido desde la detección de una anomalía en sistemas críticos (como la red de recaudo Oyster o portales de reporte de crímenes) hasta su contención y resolución definitiva. Un MTTR reducido es vital para minimizar el impacto en la disponibilidad del servicio de transporte.
- **Integridad de la Evidencia Digital:** Porcentaje de grabaciones de CCTV y dispositivos Body Worn Video (BWV) que mantienen su integridad y trazabilidad técnica, asegurando su validez como prueba forense ante la British Transport Police.
- **Eficacia de los Controles de Acceso:** Monitorización de intentos de acceso no autorizados a bases de datos sensibles, como los registros de la línea Sarah Hope o el sistema de Violencia Laboral (WVA).

Proceso de Auditoría Interna

El proceso de auditoría interna se constituye como una evaluación independiente y sistemática para verificar la conformidad del SGSI.

- **Frecuencia:** Se establece un ciclo de auditorías semestrales para sistemas de alta criticidad (transaccionales y de seguridad pública) y anuales para procesos administrativos de soporte.
- **Metodología:**
    - **Revisión de Logs:** Análisis técnico de las trazas de auditoría para verificar la trazabilidad de los accesos a sistemas de reporte de incidentes y conducta antisocial.
    - **Entrevistas:** Evaluación del nivel de concienciación del personal de campo y oficiales de Transport Support and Enforcement (TSE) respecto al manejo de datos sensibles.
    - **Pruebas de Cumplimiento en Campo:** Verificaciones físicas en estaciones y centros de control para validar la seguridad perimetral de los racks de comunicaciones y la correcta operación de los dispositivos de videovigilancia.
- **Independencia:** Para garantizar la imparcialidad, los auditores son seleccionados de departamentos ajenos al área evaluada; por ejemplo, el equipo de Seguridad Física puede auditar los protocolos lógicos de TI, asegurando que no existan conflictos de interés en los hallazgos.

Revisión por la Dirección

La alta dirección de TfL asume la responsabilidad de revisar periódicamente el SGSI para asegurar su idoneidad y eficacia continua.

- **Reportes Trimestrales:** Se generan informes técnicos de desempeño que se presentan formalmente ante el Panel de Seguridad, Sostenibilidad y RR.HH.. Este panel, que ya supervisa los esfuerzos para eliminar la violencia laboral, actúa como el máximo organismo de gobernanza del SGSI.
- **Contenido de la Revisión:** El reporte debe incluir el estado de las acciones de revisiones anteriores, cambios en los riesgos externos e internos, resultados de las auditorías y el grado de cumplimiento de los objetivos de seguridad.
- **Alineación Estratégica:** Esta revisión garantiza que el SGSI evolucione en paralelo con las necesidades de la red de transporte de Londres, asegurando que la protección de datos siga siendo un pilar habilitador para la seguridad física de los pasajeros y el personal bajo el marco de "Vision Zero".

8. Mejora Continua

La mejora continua en Transport for London (TfL) es el mecanismo operativo que garantiza que el SGSI evolucione al mismo ritmo que las amenazas tecnológicas y las necesidades de la red de transporte. Este proceso es fundamental para mantener la resiliencia de los sistemas que soportan la iniciativa "Vision Zero", asegurando que la protección de datos sea un pilar dinámico y no estático dentro de la organización.

Gestión de No Conformidades

TfL establece un procedimiento técnico riguroso para la identificación y resolución de no conformidades, entendidas como cualquier incumplimiento de los requisitos de la norma ISO 27001 o de las políticas internas de seguridad.

- **Detección e Investigación:** Ante un fallo en los controles —como una pérdida de integridad en los logs de CCTV, una vulnerabilidad no parcheada en los sistemas de recaudo Oyster o un acceso no autorizado a datos de la línea Sarah Hope— se activa un protocolo de investigación. Este incluye un Análisis de Causa Raíz (RCA) para determinar si el fallo fue de origen técnico, humano o procedimental.
- **Acciones Correctivas:** Una vez identificada la causa, se implementan acciones correctivas diseñadas para eliminar el origen del problema y prevenir su recurrencia. Por ejemplo, si una brecha de datos ocurrió por falta de segmentación de red en una estación, la acción correctiva implicará la reconfiguración técnica de los nodos de comunicación.
- **Registro y Seguimiento:** Todas las no conformidades y las medidas tomadas se documentan en un registro centralizado, el cual es revisado por el Panel de Seguridad y Sostenibilidad para validar la efectividad de las soluciones aplicadas.

Ciclo PDCA (Plan-Do-Check-Act)

TfL aplica el modelo PDCA para asegurar que el SGSI sea un sistema adaptativo capaz de hacer frente a la evolución de las ciberamenazas, especialmente aquellas dirigidas a los Sistemas de Transporte Inteligente (ITS) y la infraestructura conectada.

- **Plan (Planificar):** En esta fase, TfL identifica nuevas amenazas asociadas a proyectos de modernización, como la actualización de la línea Piccadilly o la implementación de "Safer Junctions". Se definen objetivos de seguridad que contemplan la protección de los datos generados por sensores de tráfico y sistemas de control automatizado.
- **Do (Hacer):** Se ejecutan los controles seleccionados, como el cifrado de comunicaciones en la red de autobuses o la actualización de los protocolos de seguridad en los terminales de pago. Aquí se integra la formación del personal operativo en nuevas herramientas de defensa digital.
- **Check (Verificar):** A través de las auditorías internas y el seguimiento de KPIs (como el tiempo de detección de intrusiones en la red), TfL mide si el SGSI está cumpliendo con su función de proteger la integridad del transporte público y la privacidad de los usuarios.
- **Act (Actuar):** Basándose en los resultados de la verificación, la dirección de TfL realiza ajustes estratégicos. Esto puede incluir la adopción de nuevas tecnologías de defensa contra ataques avanzados (ej. ataques dirigidos a sistemas de señalización o infraestructura de red inteligente) o el endurecimiento de las políticas de acceso tras un incidente.

9. Control de Documentación

El control documental en Transport for London (TfL) garantiza que la información que sustenta el SGSI sea precisa, esté actualizada y sea accesible únicamente para las partes autorizadas. Dada la naturaleza de TfL como organismo público encargado de infraestructuras críticas, la integridad de su documentación es un requisito indispensable para la transparencia institucional y el cumplimiento normativo.

9.1. Creación y Actualización

Se establecen estándares rigurosos para la gestión del ciclo de vida de los documentos del SGSI, asegurando la uniformidad y la trazabilidad en toda la organización:

- **Estándares de Formato:** Todos los documentos normativos, técnicos y operativos deben seguir una estructura estandarizada que incluya encabezados de control de cambios, metadatos de clasificación de seguridad y registros de autoría.
- **Proceso de Revisión y Aprobación:** La actualización de políticas y manuales técnicos debe someterse a revisiones periódicas. En el caso de documentos que impacten la seguridad operativa o la protección del personal (WVA), la aprobación final debe involucrar al Panel de Seguridad, Sostenibilidad y RR.HH. para asegurar la alineación con los objetivos estratégicos de seguridad y salud.
- **Control de Versiones:** Se implementa un sistema de control de versiones estricto para evitar el uso de documentación obsoleta en centros de control de tráfico o estaciones, garantizando que los procedimientos de respuesta ante incidentes y las guías de reporte sean siempre los vigentes.

9.2. Control de Archivos

El control de los registros en TfL es crítico debido a la alta sensibilidad de los datos recolectados y la necesidad de cumplir con obligaciones legales y de transparencia.

- **Retención de Datos de CCTV:** Las imágenes capturadas por la red de videovigilancia y dispositivos corporales (Body Worn Video) se gestionan bajo políticas de retención temporal estrictas. Conforme a las directrices operativas de TfL, los datos de CCTV se conservan únicamente por un periodo de tiempo limitado, a menos que sean requeridos como evidencia forense por la British Transport Police o para investigaciones internas tras incidentes graves.
- **Registros de Incidentes y Datos Sensibles:** Los informes de crímenes, incidentes de seguridad ciudadana y registros de atención a víctimas (como los gestionados por la línea Sarah Hope) deben custodiarse bajo medidas de seguridad reforzadas. Su retención y disposición final se ajustan a lo estipulado por el Reglamento General de Protección de Datos (GDPR) y la legislación de transporte vigente.
- **Alineación con el "Compromiso de Apertura":** El control de archivos facilita la transparencia institucional. La organización debe asegurar que los registros de seguridad vial y estadísticas de colisiones estén disponibles para el análisis de datos que impulsa la iniciativa "Vision Zero", garantizando que la información de carácter personal sea anonimizada o protegida para cumplir con la honestidad debida a los familiares y al público tras incidentes graves.