DOSSIER DE SEGURIDAD Y CUMPLIMIENTO

Seguridad, soberanía del dato y cumplimiento normativo

Arquitectura de seguridad del sistema, conformidad con TS 50701 y EN 50155, gestión de identidad, soberanía del dato del operador y cumplimiento del Reglamento Europeo de IA (AI Act) y RGPD.

Documento	IN-SIGHT-SC-001 · Versión pública 1.0
Fecha	Junio 2026
Organización	Ingérop España — División de Transportes (T3)
Programa	IN³ Season IV
Audiencia	Direcciones técnicas, responsables de ciberseguridad (CISO), DPO, asesoría jurídica

1. La seguridad empieza en la arquitectura: no intrusividad

La decisión de diseño más importante de IN-SIGHT desde el punto de vista de la seguridad no es una contramedida: es la propia arquitectura. El sistema **no se conecta a ningún bus de datos del vehículo** (MVB, CANbus, Ethernet vehicular), no accede al TCMS ni a ningún ordenador de a bordo, y opera con alimentación y comunicaciones completamente independientes. La consecuencia directa: la superficie de ataque hacia los sistemas de control, tracción, freno o señalización del vehículo es **cero por construcción**. No existe ruta física ni lógica desde IN-SIGHT hacia ningún sistema de seguridad funcional.

> **Implicación para la homologación**
> Al no modificar ni interactuar con ningún sistema certificado, la instalación de IN-SIGHT no altera el expediente de certificación de seguridad funcional del vehículo. El kit tiene la consideración de equipamiento embarcado independiente, lo que simplifica drásticamente la evaluación de riesgo del operador y elimina el principal bloqueante de adopción de las soluciones de monitorización integradas.

2. Conformidad con normativa ferroviaria

Norma	Ámbito	Aplicación en IN-SIGHT
TS 50701	Ciberseguridad en aplicaciones ferroviarias	La arquitectura se diseña conforme a TS 50701 desde el primer día: segmentación de zonas y conductos, gestión de vulnerabilidades, y trazabilidad de eventos de seguridad. Diseñado para evolucionar hacia la futura EN 50701.

Norma	Ámbito	Aplicación en IN-SIGHT
EN 50155	Equipos electrónicos embarcados en material rodante	Selección de componentes, rangos térmicos, ensayos de vibración y choque, y conectores industriales M12 conforme a la norma. Plan de certificación formal financiado con los primeros despliegues comerciales.
EN 13715	Perfiles de rueda	Referencia para las condiciones de validez del protocolo Golden Run (tolerancias de rodadura certificadas por el operador).
EMC ferroviaria	Compatibilidad electromagnética	Criterio de aceptación del piloto: cero interferencias con sistemas de señalización y comunicaciones. Digitalización de señal en origen (ESP32-S3 en pod) para minimizar cableado analógico susceptible a EMI.

3. Cifrado extremo a extremo

Estado del dato	Protección	Detalle
En tránsito	TLS 1.3	Toda comunicación del sistema: MQTT del pod al cloud, consultas del dashboard y del portal, y tráfico interno entre servicios cloud. Suites de cifrado modernas, sin downgrade.
En reposo	AES-256	Cifrado automático de todo dato almacenado (Storage Service Encryption). Soporte de claves gestionadas por el cliente (CMK) en Azure Key Vault para operadores que lo requieran.
Claves y certificados	Azure Key Vault	Ciclo de vida completo de certificados de dispositivo y claves de cifrado en módulo gestionado, con rotación y auditoría de acceso.

Cada dispositivo embarcado se autentica individualmente ante la plataforma con identidad propia y credenciales revocables por unidad: el compromiso hipotético de un kit no afecta al resto de la flota.

4. Identidad, acceso y aislamiento entre operadores

- **Microsoft Entra ID B2B** como proveedor de identidad: el personal del operador accede con sus propias cuentas corporativas Microsoft, sin credenciales adicionales que gestionar ni contraseñas compartidas. El alta y baja de personal se hereda automáticamente de la gestión de identidad del propio operador.
- **Autenticación multifactor (MFA) obligatoria** para todo acceso humano a la plataforma.
- **Control de acceso por roles (RBAC)**: perfiles diferenciados de visualización, operación de mantenimiento y administración, con privilegio mínimo por defecto.
- **Row-Level Security (RLS)** en la capa de presentación: en despliegues multi-operador, cada organización ve única y exclusivamente los datos de su flota. El aislamiento se aplica en la capa de datos, no en la de interfaz.
- **Registro auditable**: toda acción con efecto sobre el sistema —reconocimiento y cierre de alertas, aprobación de baselines, cambios de umbral— queda registrada con usuario, fecha y comentario.

5. Soberanía del dato

A diferencia de los portales de diagnóstico propietarios de los fabricantes —donde la telemetría del vehículo queda en manos del OEM—, en IN-SIGHT **el dato pertenece al operador**. Es uno de los pilares de la propuesta de valor y se materializa en compromisos concretos:

Compromiso	Materialización
Propiedad del dato	La telemetría generada por la flota del operador es propiedad del operador. Ingérop actúa como encargado del tratamiento del servicio, no como propietario del dato.

Compromiso	Materialización
Residencia en la UE	Infraestructura cloud desplegada en regiones de la Unión Europea, con residencia de datos garantizada contractualmente.
Portabilidad	Exportación de cualquier serie temporal en formatos estándar (CSV) en todo momento. Sin lock-in de datos: el histórico es del operador también al término del contrato.
Opción on-premise	La arquitectura, definida como infraestructura como código, admite despliegue en el cloud privado del operador para los casos que lo requieran.

6. Cumplimiento del Reglamento Europeo de IA (AI Act)

IN-SIGHT incorpora los principios del AI Act **por diseño**, no como adaptación posterior. El sistema de diagnóstico es deliberadamente híbrido —modelo físico riguroso más aprendizaje automático explicable— precisamente para evitar el comportamiento de caja negra:

- **Explicabilidad nativa.** La primera etapa de diagnóstico es un modelo físico (filtro de Kalman) cuya salida tiene interpretación estadística directa; la segunda emplea árboles de decisión con análisis de contribución por característica. Cada alerta puede explicarse: qué sensor, qué desviación, respecto a qué condición de referencia.
- **Trazabilidad e integridad.** Huella criptográfica SHA-256 de modelos y datasets de calibración: cada decisión del sistema es trazable a la versión exacta del modelo y del baseline que la produjo.
- **Supervisión humana efectiva.** El sistema recomienda; decide el equipo de mantenimiento. El flujo de reconocimiento y cierre de alertas con diagnóstico final mantiene al humano en el circuito y genera además el registro de verdad-terreno que mejora el sistema.
- **Gestión de riesgo proporcionada.** IN-SIGHT es una herramienta de apoyo al mantenimiento, sin función de seguridad: no actúa sobre el vehículo ni sustituye ninguna inspección reglamentaria. Su clasificación de riesgo bajo el AI Act es, en consecuencia, limitada.

7. Protección de datos personales (RGPD)

La posición de IN-SIGHT ante el RGPD es simple y robusta: **el sistema no captura datos personales**. La telemetría es exclusivamente de máquina —vibración, temperatura, acústica de componentes mecánicos, posición del vehículo—. No hay cámaras, no hay micrófonos de cabina orientados a personas, no hay datos de pasajeros ni de conducción individual. Los únicos datos de carácter personal del servicio son las cuentas de usuario del personal autorizado (nombre y correo corporativo), tratadas conforme al RGPD con finalidad exclusiva de control de acceso y auditoría. Para cada despliegue se aporta el anexo de tratamiento correspondiente y, si el operador lo requiere, la evaluación de impacto conjunta.

8. Resiliencia operativa

Escenario	Comportamiento del sistema
Pérdida de cobertura celular (túneles, zonas de sombra)	Buffer local de semanas de capacidad en el gateway embarcado. Sincronización retroactiva automática al recuperar conectividad (store-and-forward). Sin pérdida de datos.
Fallo de un sensor	Detección automática por la propia monitorización de calidad de señal; alerta al administrador. El diagnóstico continúa con las modalidades restantes con la incertidumbre correspondiente declarada.
Compromiso de un dispositivo	Revocación individual de la identidad del dispositivo sin afectar al resto de la flota. Re-aprovisionamiento con credenciales nuevas.
Indisponibilidad cloud	Los kits continúan capturando y almacenando en local. El servicio se restablece sin intervención en campo.

Para una revisión de seguridad detallada con su equipo (CISO, DPO, dirección técnica), solicite una sesión técnica en **in3-insight.cloud**.