Dirección de Transformación Digital y Tecnología

Concurso de Proyectos IA – Prevención de grafitis

Junio 2025

Anexo 1: Prevención de grafitis

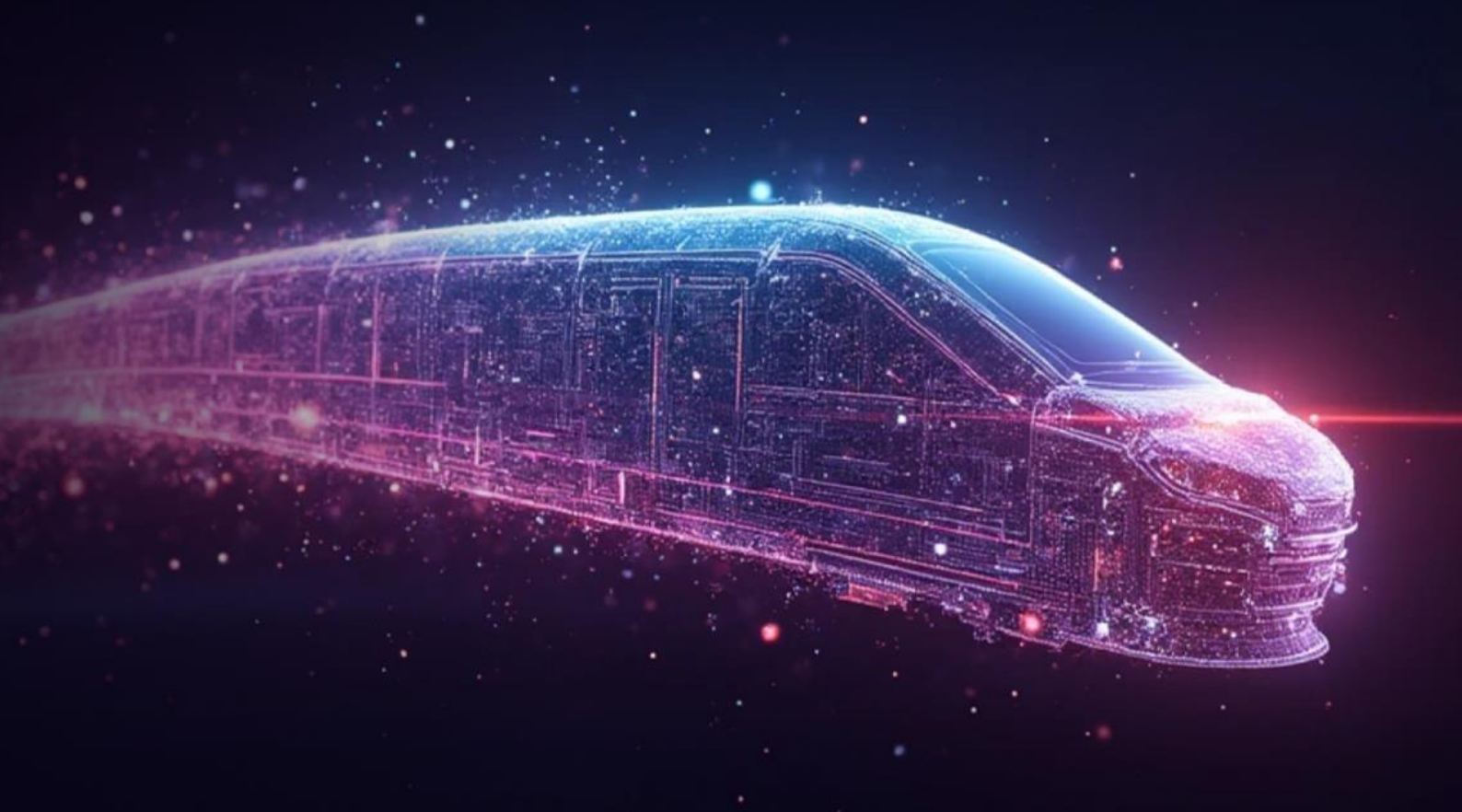

Tabla de contenido

1 Objetivos y resultados esperados

1.1 Definición del objetivo del proyecto

La propuesta de **Prevención de grafitis mediante IA** tiene como objetivo desarrollar un sistema predictivo capaz de anticipar, disuadir y reducir significativamente los actos de vandalismo sobre trenes e instalaciones, con especial foco en los ataques mediante grafiti. Esta iniciativa se enmarca en el compromiso de RENFE por reforzar la disponibilidad del material rodante para mejorar el servicio ofrecido a los clientes, así como, aumentar la seguridad, optimizar los recursos de vigilancia y proteger su imagen corporativa.

Nivel táctico-operativo

Desde una perspectiva operativa, el objetivo es dotar a los equipos de seguridad y operación de una **herramienta de apoyo a la decisión basada en IA**, que permita:

- **Analizar el histórico de incidentes** de grafitis (ubicación, tipo de ataque, día y hora, contexto del suceso) para identificar patrones de comportamiento recurrentes.
- **Generar alertas predictivas en tiempo real**, con al menos dos horas de antelación, que señalen zonas y franjas horarias de **alto riesgo de vandalismo**.
- Activar mecanismos de **visión artificial en cámaras existentes** para detectar movimientos sospechosos o actividades anómalas en cocheras, estaciones y tramos vulnerables.
- **Sugerir la priorización dinámica de rondas de vigilancia**, permitiendo una asignación óptima de recursos humanos y técnicos.

Todo ello se orienta a prevenir la acción antes de que ocurra, reduciendo la necesidad de intervenir tras el daño ya realizado.

Nivel estratégico

A nivel estratégico, el proyecto responde al reto de:

- Evolucionar desde un modelo **reactivo (limpieza posterior al daño)** hacia un modelo **predictivo y preventivo**, más eficiente y sostenible.
- Aportar valor a los **objetivos corporativos de disponibilidad y mejora de experiencia de cliente**, al permitir que más unidades estén en operación en lugar de fuera de servicio por limpieza.
- **Proteger la reputación e imagen de marca de RENFE**, reduciendo la exposición de trenes vandalizados a la vista del cliente.
- Contribuir a los objetivos del Plan Estratégico y de la Agenda de Transformación Digital 2025, posicionando a RENFE como una operadora pionera en el uso de IA para la seguridad ferroviaria.

Nivel cultural

A nivel cultural, se busca un cambio de paradigma en la forma en que se aborda la prevención del vandalismo:

- **Dotar al personal de seguridad y operaciones** de herramientas de análisis de datos e inteligencia artificial que complementen la experiencia operativa.

- Fomentar una **cultura proactiva y basada en evidencias**, donde las decisiones se apoyen en modelos de predicción y análisis automatizado.
- Reforzar la **colaboración transversal entre Seguridad, Operaciones, Mantenimiento y Tecnología**, generando una dinámica de trabajo más coordinada y ágil.
- Posicionar la lucha contra el grafiti como un **objetivo colectivo, visible y medible**, generando orgullo interno al reducir de forma tangible una de las problemáticas más costosas y visibles para la organización.

Principios rectores del proyecto

Este proyecto se regirá por una serie de principios operativos y éticos que garantizarán su viabilidad y sostenibilidad:

1. **Enfoque preventivo desde el diseño**: introducir la disuasión y anticipación para reducir la limpieza y reparación.
2. **IA explicable (XAI)**: asegurar que los modelos generen decisiones interpretables para los usuarios finales.
3. **Uso de infraestructura existente**: reutilizar cámaras, sistemas de seguridad y datos históricos sin necesidad de grandes inversiones adicionales.
4. **Escalabilidad modular**: comenzar con una **POC en zonas de alta incidencia** (ej. cocheras críticas o tramos urbanos) y escalar progresivamente según resultados.
5. **Cumplimiento normativo**: integración con las políticas de privacidad y ciberseguridad de RENFE, incluyendo el tratamiento ético y anónimo de las imágenes y datos recogidos.
6. **Medición y mejora continua**: establecer KPIs desde el inicio que permitan evaluar el impacto y realimentar los modelos de IA con cada nuevo incidente registrado.

Síntesis del objetivo

Diseñar, desarrollar y validar un **sistema de IA predictivo y preventivo** que permita anticipar ataques de grafiti sobre trenes e instalaciones mediante el análisis histórico de incidentes, visión artificial sobre cámaras ya instaladas y generación automatizada de alertas, con el fin de **reducir en un 20 % los incidentes detectados** y al menos un **15 % el tiempo medio de inactividad por limpieza** durante el piloto inicial.

1.2 Problemática o necesidad específica a resolver

Contexto general

El vandalismo mediante **grafitis no autorizados** representa un desafío operativo, económico y reputacional para RENFE. Solo en el año 2024, este tipo de actos ha generado **más de 11 millones de euros en costes directos**, entre limpiezas, reparación de daños y pérdida de disponibilidad de trenes. Este impacto económico se suma a un deterioro en la **percepción del servicio por parte del viajero** y a un problema creciente de seguridad.

Los grafitis no solo afectan al material rodante, sino también a instalaciones como cocheras, túneles y estaciones. Además, se han observado nuevas tácticas más agresivas y organizadas por parte de los atacantes, incluyendo el uso del **freno de emergencia ("palancazo")** para forzar la detención del tren y ejecutar el acto vandálico.

Este fenómeno ha evolucionado de actos esporádicos a **acciones planificadas por grupos organizados**, que operan con información previa sobre la ubicación de los trenes, la vigilancia presente y las condiciones contextuales del entorno.

Problemáticas clave que el proyecto busca resolver

1. **Reacción tardía**: En la actualidad, las acciones frente al grafiti se realizan de forma reactiva, una vez que el daño ya está hecho.
2. **Costes operativos acumulados**: La limpieza y reparación afectan directamente la operativa, ya que los trenes deben ser retirados del servicio, incrementando costes y afectando la disponibilidad de flota.
3. **Despliegue de vigilancia no optimizado**: Las patrullas de seguridad no siempre se orientan a las zonas de mayor riesgo en el momento adecuado.
4. **Falta de herramientas predictivas**: No se dispone actualmente de un sistema capaz de anticipar ataques a partir del análisis de datos históricos, contexto ambiental o patrones de comportamiento.
5. **Dificultad para detectar nuevas tácticas**: Las estrategias como el "palancazo" requieren una **reacción anticipada** que hoy no es posible sin capacidades predictivas o de análisis en tiempo real.

Oportunidad: una transformación estratégica de la gestión de la información operativa

La situación descrita pone de manifiesto la necesidad de **migrar desde un modelo reactivo hacia un modelo proactivo** y basado en datos. La aplicación de inteligencia artificial (IA) en este contexto representa una **oportunidad estratégica** para transformar la forma en que RENFE gestiona los riesgos asociados al grafiti:

- Aprovechando los **datos históricos** y datos del contexto externo (climatología, eventos, etc.) para extraer patrones de comportamiento y zonas de riesgo.
- Integrando variables contextuales como hora, clima o eventos próximos para **anticipar** posibles ataques.
- Incorporando **visión artificial** básica sobre cámaras existentes para detectar presencia sospechosa o intentos de vandalismo.
- Generando **alertas proactivas** que orienten las patrullas de vigilancia de forma más eficiente y efectiva.

Esta propuesta no solo aborda el problema desde la tecnología, sino que se enmarca en una estrategia más amplia de **protección del servicio público, optimización de recursos operativos y mejora continua de la seguridad ferroviaria**.

1.3 Hipótesis clave que validarán la PoC

El desarrollo del sistema predictivo para la prevención de actos vandálicos en trenes e instalaciones implica la validación de un conjunto de hipótesis que permitirán confirmar la viabilidad funcional y tecnológica del enfoque propuesto. Estas hipótesis se organizan en dos bloques principales:

- **Hipótesis funcionales**, centradas en demostrar la utilidad práctica de las alertas y recomendaciones para la prevención de grafitis en el entorno real.
- **Hipótesis tecnológicas**, enfocadas en evaluar la capacidad del sistema para integrarse, generar resultados de forma eficiente y escalar a futuro dentro del ecosistema técnico de RENFE.

A. Hipótesis funcionales

Estas hipótesis buscan demostrar que el sistema contribuye a mejorar la prevención, intervención y asignación de recursos frente a actos vandálicos.

Hipótesis	Descripción	Validación esperada
H01 – Capacidad predictiva	El sistema puede anticipar al menos el 50 % de los incidentes registrados en zonas piloto con un margen de ≥ 2 horas.	Comparación entre alertas emitidas y registros reales de incidencias durante el piloto.
H02 – Utilidad operativa de las alertas	Al menos el 75 % de las alertas emitidas son percibidas como útiles o muy útiles por los equipos de vigilancia.	Encuesta post-ronda a personal de seguridad en las zonas piloto.
H03 – Reducción de incidentes	Las zonas piloto con despliegue basado en alertas presentan una reducción ≥ 20 % de grafitis respecto a zonas sin intervención.	Comparativa de datos históricos vs. datos durante el piloto en zonas control y tratamiento.
H04 – Optimización de rondas de vigilancia	El sistema permite optimizar las rondas semanales, reduciendo desplazamientos innecesarios o reforzando zonas de alto riesgo.	Análisis de cambios en los recorridos realizados y validación con los responsables de seguridad.
H05 – Impacto en el tiempo de inactividad	La prevención efectiva disminuye el tiempo de inactividad de los trenes por tareas de limpieza.	Evaluación comparativa de horas de inmovilización antes y durante el piloto en zonas seleccionadas.

B. Hipótesis tecnológicas

Las hipótesis tecnológicas evaluarán la capacidad del sistema para operar de forma robusta y eficiente en el entorno real, con una arquitectura sencilla y escalable.

Hipótesis	Descripción	Validación esperada
H06 – Integración de datos históricos	El sistema puede integrar y procesar correctamente datos históricos de incidencias con al menos 2 años de cobertura.	Validación de calidad y cobertura de datos disponibles. (Completar con ayuda de RENFE: fuentes internas y formatos actuales)
H07 – Enriquecimiento contextual	Es posible enriquecer los datos con variables externas relevantes (clima, eventos, calendario) sin desarrollo adicional complejo.	Confirmación de la integración básica de datos contextuales y evaluación de su utilidad predictiva.
H08 – Generación de alertas con latencia baja	El sistema es capaz de generar alertas automáticas con una latencia < 10 min desde la detección de condiciones de riesgo.	Medición del tiempo de procesamiento de eventos y emisión de alertas en entorno piloto.

H09 – Visualización operativa básica	El sistema puede representar visualmente las zonas de riesgo en mapas de calor y calendarios temporales sin necesidad de herramientas externas complejas.	Validación de las visualizaciones con usuarios operativos y responsables de vigilancia.
H10 – Escalabilidad técnica inicial	La solución puede extenderse a nuevas zonas geográficas sin rediseño completo del modelo o arquitectura.	Prueba controlada con extensión del modelo a al menos una segunda zona con características distintas.
H11 – Seguridad de datos y cumplimiento normativo	El tratamiento de datos históricos y contextuales cumple con la normativa vigente y las políticas de seguridad de RENFE.	Revisión técnica de los mecanismos de anonimización, trazabilidad y gestión de datos. (Completar con ayuda de RENFE: requisitos internos de cumplimiento y GDPR)

Nota metodológica:

La validación de estas hipótesis se realizará a través de una combinación de métodos cualitativos y cuantitativos, incluyendo:

- Análisis retrospectivo y comparativo de incidencias reales.
- Encuestas a personal operativo y supervisores.
- Medición directa de rendimiento del sistema.
- Pruebas piloto controladas en zonas de alta incidencia.
- Feedback iterativo con stakeholders clave de RENFE Seguridad.

1.4 Resultados esperados y métricas clave (KPIs)

El desarrollo de la PoC del sistema de prevención de grafitis mediante analítica predictiva e inteligencia artificial tiene como objetivo demostrar su capacidad para **reducir los actos vandálicos**, **optimizar la vigilancia operativa** y **minimizar los costes derivados de la limpieza y la inactividad de los trenes**.

El sistema se plantea como un **asistente estratégico a la toma de decisiones**, que ayuda a los equipos de seguridad a anticiparse a incidentes a partir de patrones detectados en datos históricos, contexto operativo y vídeo vigilancia.

Durante el piloto, se evaluará su valor mediante un conjunto de **indicadores clave de rendimiento (KPIs)** definidos a continuación.

Resultados esperados

- **Reducción del número de grafitis** mediante la anticipación a patrones de ataque.
- **Disminución del tiempo medio de limpieza** y reposición del tren tras un acto vandálico.
- **Generación de alertas predictivas** con una antelación suficiente para la activación preventiva de recursos de seguridad.
- **Reasignación dinámica de rondas de vigilancia**, priorizando zonas y horarios de alto riesgo.
- **Ahorro económico directo e indirecto**, especialmente en limpieza, horas de inactividad y reprogramaciones.

- **Mayor aceptación por parte de los equipos operativos**, al contar con una herramienta intuitiva, útil y explicable.

KPIs

Categoría	Indicador	Objetivo / Métrica esperada
Eficiencia operativa	Disminución de actos vandálicos en zonas piloto	≥ 20 % de reducción respecto al histórico
	Tiempo medio de inactividad por limpieza tras incidente	Mejora del 15 % respecto a 2023
	% de alertas emitidas con ≥ 2h de antelación	≥ 50 % de alertas con antelación suficiente para activar patrulla
	Rondas de vigilancia replanificadas dinámicamente	≥ 25 % de las rondas ajustadas por el sistema
Calidad de las predicciones	Tasa de acierto de las alertas (precisión)	≥ 70 %
	Falsos positivos por semana	≤ 2 por zona
Impacto económico estimado	Ahorro estimado en limpieza y logística	≥ 150.000 € anualizados
	Reducción del coste por hora de inactividad de trenes	≥ 10 % de mejora
Aceptación y experiencia del usuario	Nivel de satisfacción del personal de seguridad	≥ 80 % en encuestas post-uso
	Percepción de utilidad de las alertas en la operativa real	≥ 75 % consideran las alertas útiles
Escalabilidad y viabilidad técnica	N° de fuentes de datos integradas en tiempo real	≥ 3 fuentes clave (histórico, cámaras, contexto externo) *(Completar con ayuda de RENFE: especificar sistemas)*
	Tiempo de despliegue en nueva ubicación	< 3 días por cochera o zona

2 Alcance funcional del proyecto (POC)

2.1 Funcionalidades incluidas en la primera versión (POC)

La PoC del sistema de prevención de grafitis se enfoca en generar valor desde la fase más temprana mediante el uso inteligente de datos históricos y contextuales. Durante las primeras 8-10 semanas, el desarrollo se centrará en funcionalidades que permitan identificar patrones de riesgo horario y geográfico, generar alertas preventivas y sugerir acciones operativas basadas en datos, sin entrar aún en la fase de análisis de vídeo en tiempo real.

Las funcionalidades incluidas en esta primera versión son las siguientes:

A. Ingesta y enriquecimiento de datos históricos

- **Integración de la base de datos histórica de incidentes de grafitis**, incluyendo variables clave como fecha, hora, localización, tipo de ataque, entorno (cochera, vía, estación), duración e impacto operativo (tiempo de inactividad, unidades afectadas).
- **Enriquecimiento contextual automático** con datos de fuentes externas, como:
  - Condiciones meteorológicas por franja horaria (precipitación, visibilidad, etc.).
  - Eventos públicos relevantes (festividades, conciertos, fútbol).
  - Calendario laboral y distribución por día/turno.

B. Modelado predictivo de riesgo horario-espacial

- Implementación de un **modelo de machine learning supervisado** (e.g., gradient boosting, árboles de decisión) para generar un mapa de calor predictivo que identifica zonas y horarios de mayor riesgo de ataques en las siguientes 24 horas.
- El modelo se entrenará con históricos anonimizados y será capaz de actualizarse diariamente, incorporando los últimos incidentes reportados para mejorar su precisión progresivamente.

C. Visualización operativa del riesgo

- Desarrollo de un **dashboard web de visualización dinámica**, accesible por personal de seguridad y análisis operativo, con:
  - Mapa de calor de riesgo por tramo horario y ubicación.
  - Ranking de zonas críticas (Top-10) y evolución temporal.
  - Exportación semanal de predicciones y rendimiento del sistema.

D. Generación de alertas tempranas y sugerencias de acción

- Sistema de alertas configurables que, en función de los niveles de riesgo definidos, notificará a los responsables de vigilancia por correo electrónico o canal interno (Teams u otro).
- El sistema incluirá un **módulo de sugerencia de patrullaje**, que reorganiza de manera priorizada la ronda nocturna habitual para incorporar las zonas más críticas, sin modificar los sistemas oficiales de planificación.

E. Registro y retroalimentación del usuario

- Herramienta sencilla para que el personal operativo pueda registrar si un ataque se produjo o no en una zona alertada, facilitando el cálculo de precisión del modelo (falsos positivos/negativos).
- Este registro de feedback será clave para reentrenar el modelo y mejorar su rendimiento en fases futuras.

2.2 Requerimientos funcionales

Para garantizar que la PoC del sistema de prevención de grafitis cumpla con sus objetivos operativos, se definen los siguientes **requerimientos funcionales clave**. Estos requisitos se centran en asegurar la ingesta de datos históricos, la generación de modelos predictivos, la visualización útil de los resultados y la capacidad de operar de forma autónoma y trazable en el entorno de RENFE.

1. Ingesta y estructuración de datos históricos

- El sistema debe permitir **importar y procesar datos históricos de incidentes** de grafitis, incluyendo:
  - Fecha y hora del incidente.
  - Localización geográfica (cochera, estación, vía).
  - Tipo de ataque (graffiti exterior, intrusión por palancazo, etc.).
  - Tiempo de inactividad y costes estimados.
- Los datos deben poder ser estructurados en un formato normalizado que permita su análisis temporal y geoespacial.

2. Enriquecimiento de contexto externo

- El sistema debe integrarse con fuentes externas (API públicas o bases de datos internas) para enriquecer los incidentes históricos con:
  - Información meteorológica (por ubicación y franja horaria).
  - Eventos públicos o actividades anómalas.
  - Calendario laboral o patrones por días especiales.
- La actualización de estos datos debe realizarse como mínimo una vez por día.

3. Modelado predictivo del riesgo

- El sistema debe ser capaz de:
  - Generar modelos de riesgo horario-espacial a partir del histórico, usando técnicas de aprendizaje supervisado.
  - Actualizar los modelos de forma periódica (mínimo semanal), incorporando los nuevos datos recogidos por el usuario.
  - Calcular métricas básicas de rendimiento del modelo (precisión, recall, tasa de falsos positivos).

4. Visualización operativa del riesgo

- El sistema debe ofrecer una interfaz web accesible desde intranet RENFE con las siguientes capacidades:
  - Visualización de mapa de calor de riesgo por zona y hora.
  - Lista de zonas más críticas para el día siguiente.

- Evolución de la predicción histórica y validación del modelo.

5. Alertas automatizadas

- El sistema debe generar alertas automáticas diarias dirigidas a los responsables de seguridad, incluyendo:
  - Descripción del riesgo (zona, franja horaria).
  - Nivel de prioridad asignado (alto, medio, bajo).
  - Sugerencia de ajuste en rondas o patrullas de vigilancia.
- Las alertas deben enviarse mediante correo electrónico o canales internos (por ejemplo, Teams o panel).

6. Módulo de validación y retroalimentación

- El sistema debe permitir al usuario operativo:
  - Confirmar si un incidente ocurrió en una zona alertada.
  - Añadir observaciones cualitativas sobre patrullaje, errores o falsas alarmas.
- Esta funcionalidad es clave para la mejora continua del modelo en fases futuras.

2.3 Requerimientos no funcionales

El desarrollo de la PoC de prevención de grafitis requiere garantizar una serie de condiciones no funcionales que aseguren su viabilidad técnica, su integración con el ecosistema tecnológico de RENFE y su utilidad en contexto operativo real. A continuación, se detallan los **requerimientos no funcionales clave** para esta primera fase del proyecto:

1. Disponibilidad y operatividad

- El sistema debe estar disponible en modalidad **cloud (nube)** con acceso desde intranet o red segura de RENFE, garantizando una operatividad mínima del **99%** durante los turnos operativos clave.
- No se requerirá una arquitectura de alta disponibilidad ni recuperación automática ante desastres, dado que la PoC no tendrá carácter crítico en esta fase.

2. Seguridad de la información

- Todos los datos gestionados por el sistema (históricos y enriquecidos) deben mantenerse cifrados en tránsito mediante **protocolo HTTPS**.
- El acceso al sistema debe realizarse mediante **autenticación corporativa** (por ejemplo, Azure Active Directory).
- No se almacenarán datos personales ni sensibles, cumpliendo con el **Reglamento General de Protección de Datos (GDPR)** y la política interna de seguridad digital de RENFE.

3. Rendimiento del sistema

- La generación de modelos y visualización de mapas no deberá superar los **30 segundos** de latencia desde la ejecución hasta la entrega de resultados, para mantener la fluidez operativa.
- Las predicciones deben estar disponibles al menos con **24 horas de antelación**, permitiendo actuar con margen suficiente sobre las zonas de riesgo.

4. Trazabilidad y explicabilidad

- El sistema debe registrar las acciones relevantes del usuario (validaciones, correcciones, observaciones), y permitir su trazabilidad para análisis posteriores.
- Toda alerta generada debe incluir una **explicación clara de los factores de riesgo** que han motivado su emisión (por ejemplo: histórico en la zona, tipo de evento, condiciones meteorológicas similares).

5. Usabilidad y autonomía del usuario

- La interfaz del sistema debe ser sencilla, **intuitiva y utilizable sin formación técnica avanzada**.
- El personal de vigilancia o responsables de seguridad deben poder utilizar el sistema sin depender de personal técnico externo, especialmente para acceder a las visualizaciones, generar informes o aportar validaciones tras los incidentes.

6. Mantenimiento y soporte

- El sistema debe requerir **soporte técnico mínimo** durante el piloto. Las actualizaciones y ajustes se realizarán por parte del equipo de desarrollo, sin impacto en el usuario final.
- No se prevé mantenimiento correctivo intensivo en esta fase, pero sí un canal habilitado para **soporte reactivo** en caso de bloqueos o errores críticos.

2.4 Limitaciones de la PoC (recursos, presupuesto, tiempo, datos)

El objetivo de la PoC del sistema de prevención de grafitis es demostrar la **viabilidad operativa y técnica** de una solución basada en inteligencia artificial (IA) para anticipar actos vandálicos en trenes e instalaciones. Dado su carácter exploratorio, esta primera fase conlleva **limitaciones explícitas** en cuanto a recursos disponibles, plazos, volumen de datos y capacidades técnicas integradas. A continuación, se detallan dichas limitaciones estructuradas por categoría:

A. Recursos

1. Personal:

- El equipo de desarrollo estará compuesto por un número reducido de profesionales especializados (científicos de datos, ingenieros de IA, analistas funcionales y diseñadores de interfaz), lo que limita la posibilidad de incorporar múltiples funcionalidades simultáneamente.
- No se contempla en esta fase la dedicación plena de equipos de vigilancia o responsables de seguridad para retroalimentar el sistema de forma continua.

2. Infraestructura:

- Uso de plataformas cloud ya contratadas por RENFE (Azure, AWS, IBM etc.) con proveedores con acuerdos existentes, o con fabricantes/proveedores con capacidad de inversión en fase de PoC para poner en valor su tecnología, minimizando de este modo gastos adicionales.
- No se instalarán nuevas cámaras ni sensores; se reutilizará el parque tecnológico ya operativo (por ejemplo, sistemas de CCTV en talleres y estaciones).

3. Capacidad operativa:

- El sistema se validará en un número **limitado de ubicaciones piloto** con alta incidencia de grafitis, y no será escalado inicialmente a toda la red.
- Las recomendaciones estarán dirigidas al **ámbito de prevención y análisis estratégico**, pero no incluirán automatismos de actuación o integración directa con protocolos operativos de intervención.

B. Presupuesto

1. Coste del desarrollo:

- Se priorizarán las funcionalidades críticas para validar las hipótesis de la POC: modelado predictivo, visualización en mapa de calor y generación de alertas básicas.
- Funcionalidades avanzadas (detección visual en vídeo en tiempo real, integración con sistemas de intervención o dashboards corporativos) **quedarán fuera del alcance de esta fase**.

2. Soporte y mantenimiento:

- El soporte técnico durante la POC será limitado a resolución de bloqueos críticos.
- No se incluyen tareas de mantenimiento evolutivo, refuerzo de infraestructura ni soporte 24/7.

C. Tiempo

1. Plazo de ejecución:

- El desarrollo completo de la PoC se realizará en un periodo máximo de **8 a 10 semanas**, lo que restringe la complejidad técnica del sistema y acota la cobertura geográfica.
- Las pruebas y ajustes serán iterativos, pero **no se contemplan ciclos amplios de validación funcional en entornos productivos reales**.

2. Entorno de despliegue:

- El sistema se implementará en un entorno de **preproducción o sandbox**, con validación por parte de un grupo reducido de usuarios.
- No se prevé su integración directa con sistemas corporativos de RENFE como SAP, Copérnico o herramientas operativas de seguridad.

D. Datos

1. Fuentes de datos:

- Se trabajará con **el histórico estructurado de incidencias por grafitis** ya recopilado por RENFE, complementado con datos contextuales externos (meteorología, eventos cercanos, horarios).
- No se integrarán fuentes audiovisuales en tiempo real ni se conectarán flujos de vídeo activos en esta fase.

2. Calidad y disponibilidad:

- Se parte del supuesto de que el histórico existente es **suficientemente representativo y etiquetado** para construir los primeros modelos predictivos.
- El enriquecimiento con datos externos dependerá de su **accesibilidad pública o mediante acuerdos mínimos de uso**, sin recurrir a licencias de terceros de alto coste.

3 Evaluación estimada de esfuerzo y recursos

3.1 Estimación de esfuerzo (en horas/hitos clave)

Con el objetivo de entregar un POC funcional en un plazo de **8 a 10 semanas**, se ha diseñado un plan de ejecución realista, concentrado en los elementos clave que permiten validar la viabilidad operativa y técnica del sistema de **prevención de grafitis**. La planificación se estructura en cinco grandes hitos, que cubren desde el diseño inicial hasta la validación final, con una estimación de esfuerzo detallada por cada fase.

Hito	Descripción	Horas estimadas
1. Diseño funcional y análisis de datos	Definición del alcance funcional de la PoC, mapeo de procesos de seguridad y limpieza, y consolidación del inventario de datos históricos (incidencias, localización, tipo de ataque). Se incluye la planificación de interacciones con los equipos de seguridad y la priorización de cocheras piloto.	80 h
2. Implementación base del sistema	Configuración técnica sobre infraestructura cloud existente, desarrollo de conectores a fuentes de datos clave (grafitis, climatología, eventos), y normalización de datos para el pipeline de procesamiento. Incluye creación del sistema de ingestión y almacenamiento básico.	320 h
3. Modelado predictivo y generación de alertas	Desarrollo de modelos de predicción de riesgo de grafitis por hora y localización (árboles de decisión, heurísticas, u otros enfoques de clasificación), junto a reglas para activar alertas tempranas en zonas críticas.	120 h
4. Interfaz de visualización operativa	Diseño y despliegue de un dashboard web para operadores de seguridad, con visualización de alertas clasificadas, mapas de calor por zonas, y herramientas básicas de validación (por ejemplo, "alerta atendida").	120 h
5. Pruebas funcionales y despliegue controlado	Validación del sistema en 1-2 cocheras piloto, medición de KPIs (tiempo de respuesta, efectividad de alertas), y soporte técnico para ajustes post-despliegue. Incluye formación básica al personal involucrado.	80 h

Total estimado de esfuerzo: 720 horas

3.2 Sugerencia de perfiles requeridos

El desarrollo de la PoC del sistema de prevención de grafitis requiere la colaboración de un equipo técnico y funcional compacto, pero altamente especializado, capaz de cubrir todas las fases del proyecto: desde la integración de datos históricos hasta el despliegue de modelos predictivos y herramientas de visualización en tiempo real. A continuación, se detallan los perfiles clave necesarios para completar la PoC en el plazo estimado de 8 a 10 semanas.

A. Coordinador funcional / Product Owner

Responsabilidades:

- Definir el alcance funcional de la PoC y priorizar funcionalidades clave.
- Facilitar la coordinación con los equipos de seguridad, operaciones y datos.
- Garantizar el alineamiento del sistema con los objetivos operativos de RENFE.
- Validar entregables funcionales y gestionar la evolución iterativa del sistema.

Habilidades requeridas:

- Conocimiento del entorno ferroviario y protocolos de seguridad.
- Experiencia previa en gestión de proyectos tecnológicos.
- Capacidad de traducir necesidades operativas en especificaciones viables.

Dedicación estimada: 25 % durante todo la PoC.

B. Ingeniero/a de datos (Backend)

Responsabilidades:

- Conectar fuentes de datos relevantes (históricos de grafitis, datos contextuales).
- Preparar pipelines para el procesamiento y almacenamiento estructurado.
- Normalizar, enriquecer y mantener actualizado el conjunto de datos del sistema.

Habilidades requeridas:

- Lenguajes como Python o Scala.
- Conocimientos en arquitecturas cloud y herramientas de ETL.
- Dominio de bases de datos relacionales y no relacionales.

Dedicación estimada: Full-time durante semanas 1–6.

C. Especialista en analítica predictiva / ML

Responsabilidades:

- Diseñar y entrenar modelos de predicción de riesgo (en función de hora, localización, patrones históricos).
- Validar precisión, interpretabilidad y utilidad de los modelos.
- Generar reglas heurísticas complementarias para la activación de alertas.

Habilidades requeridas:

- Conocimientos en aprendizaje supervisado y árboles de decisión.
- Manejo de librerías como Scikit-learn, XGBoost, Pandas.
- Capacidad de explicar los modelos a usuarios no técnicos.

Dedicación estimada: 50 % durante semanas 3–7.

D. Frontend Developer + Diseñador/a UX-UI

Responsabilidades:

- Diseñar una interfaz clara para operadores de vigilancia.
- Implementar visualizaciones (mapas de calor, cronogramas de alertas).
- Asegurar la navegabilidad y la simplicidad del uso en campo.

Habilidades requeridas:

- Frameworks como React o Vue.js.
- Diseño web responsivo y principios de accesibilidad.
- Experiencia en visualización de datos geoespaciales (opcional).

Dedicación estimada: 2 semanas intensivas (semanas 5 y 6) + soporte puntual.

E. QA / Tester funcional

Responsabilidades:

- Validar la estabilidad del sistema y la consistencia de los datos.
- Diseñar escenarios de prueba con personal de campo.
- Ejecutar validaciones funcionales del dashboard y alertas generadas.

Habilidades requeridas:

- Experiencia en testing funcional/manual.
- Capacidad de documentación clara y seguimiento de incidencias.
- Coordinación con usuarios finales en entornos operativos.

Dedicación estimada: Parcial, concentrada en semanas 7–9.

Resumen de dedicación por perfil

Perfil	Rol principal	Dedicación estimada
Coordinador funcional	Coordinación y validación	25 % continuo
Ingeniero/a de datos	Integración y preparación de datos	Full-time semanas 1–6
Especialista ML	Modelado predictivo y reglas	50 % semanas 3–7
UX-UI + Frontend	Interfaz de visualización	2 semanas intensivas

QA / Tester	Pruebas y validación	Parcial semanas 7–9

3.3 Herramientas y plataformas de IA necesarias o recomendadas

El desarrollo de la POC para la prevención de grafitis se sustentará sobre una arquitectura técnica **ligera, segura y modular**, aprovechando las capacidades tecnológicas ya disponibles en RENFE. El enfoque busca un **equilibrio entre velocidad de despliegue, escalabilidad futura y control operativo**, evitando dependencias innecesarias o inversiones anticipadas en infraestructuras complejas.

A continuación, se detallan los componentes clave que deben estar disponibles o habilitados para garantizar el funcionamiento eficaz del sistema durante la fase piloto.

A. Infraestructura cloud corporativa

Tipo de tecnología: Plataforma de nube híbrida o pública ya disponible en RENFE.
Uso previsto:

- Despliegue del sistema de alertas y los servicios asociados.
- Procesamiento del histórico de datos y de los modelos predictivos.
- Almacenamiento temporal de datos y configuración de reglas.

Observaciones:

- No se requieren entornos dedicados de alta disponibilidad.
- Se recomienda aprovechar entornos compartidos o preproductivos, si están disponibles.

B. Servicios de análisis predictivo

Tipo de tecnología: Herramientas de analítica avanzada y aprendizaje automático supervisado.
Uso previsto:

- Entrenamiento de modelos basados en el histórico de grafitis.
- Identificación de patrones por localización, franja horaria o contexto externo.
- Generación de puntuaciones de riesgo para zonas o momentos determinados.

Observaciones:

- Se prioriza la explicabilidad del modelo frente a su complejidad.
- No se contempla el uso de modelos generativos ni de aprendizaje profundo en esta fase.

C. Plataforma de visualización operativa

Tipo de tecnología: Aplicación web o sistema de dashboards para visualización interactiva.
Uso previsto:

- Representación geoespacial y temporal del riesgo por zona.
- Mapa de calor con alertas en tiempo real.
- Panel de priorización de rondas de vigilancia.

Observaciones:

- Interfaz orientada a operativos de seguridad.
- Diseño simple, claro y navegable sin formación intensiva.

D. Sistema de almacenamiento de datos estructurados

Tipo de tecnología: Repositorio centralizado para datos históricos, enriquecidos y alertas generadas.
Uso previsto:

- Consolidación del histórico de grafitis y contexto.
- Registro de alertas y validaciones operativas.
- Posible expansión hacia un módulo de aprendizaje continuo en fases posteriores.

Observaciones:

- El volumen de datos previsto durante la POC será limitado.
- Se prevé un proceso de curación manual para asegurar la calidad de la información inicial.

E. Conectores y sistemas de integración de datos

Tipo de tecnología: Interfaces de conexión a bases de datos internas, APIs y sistemas de información de seguridad.
Fuentes de datos previstas:

- Histórico de grafitis por localización, fecha y tipo de incidente.
- Datos de contexto externo (clima, eventos, horario, etc.).
- Información operativa relacionada con disponibilidad de trenes o zonas en vigilancia.

F. Módulos de autenticación y seguridad

Tipo de tecnología: Sistemas corporativos de gestión de identidad, acceso y cifrado.
Uso previsto:

- Autenticación de usuarios internos para acceso al sistema.
- Protección de datos sensibles (como localizaciones críticas o protocolos operativos).

Observaciones:

- El sistema no tratará datos personales.
- Se aplicarán los estándares de ciberseguridad definidos por RENFE para proyectos operativos.

Resumen general

Recurso	Necesidad en la PoC	Observaciones clave
Infraestructura cloud	Entorno de despliegue técnico	Preferentemente reutilización de entornos existentes
Servicios de analítica e IA	Modelado de patrones de riesgo	Enfoque supervisado, explicable, no generativo
Plataforma de visualización operativa	Panel interactivo con mapas y alertas	Interfaz pensada para operativos de seguridad
Almacenamiento de datos estructurados	Histórico y alertas	Corpus curado y de volumen limitado
Integración de datos	Fuentes operativas y de contexto	Requiere validación conjunta con CGO y TI
Seguridad y autenticación	Acceso seguro y cumplimiento normativo	Sin tratamiento de datos personales