UTE FORENSIA THOT

F1.3.3 Plan de Pruebas de Interoperabilidad

THOT

Periodo de Informe *<30/09/2025>* **a** *<27/02/2026>*

Fecha: 27/02/2026
Versión: 2.0

Información de control del documento

Descripción	Valor
Título del Documento:	Documento de Plan de Pruebas de Interoperabilidad
Nombre del Proyecto:	THOT
Autor del documento:	Sergio Zaera Mata, Sergio Queraltó Pereira, Jaime Castro Cernadas
Propietario del Proyecto:	UTE FORENSIA THOT
Director del Proyecto:	Roberto Gómez-Espinosa
Versión Doc.:	2.0
Confidencialidad:	Alta
Fecha:	27/02/2026

Aprobación y revisión del documento:

NOTA: Se requieren todas las aprobaciones. Se deben mantener registros de cada aprobación.

Todos los revisores de la lista se consideran necesarios a menos que se indique explícitamente como Opcionales.

Nombre	Rol	Acción	Fecha
Sergio Zaera Mata	Jefe de Proyecto	Revisa	26/01/2026

Historial de documentos:

El Autor del Documento está autorizado a hacer los siguientes tipos de cambios al documento sin requerir que el documento sea aprobado nuevamente:

- Editorial*, formateo y ortografía.*
- Aclaración.

Para solicitar un cambio en este documento, póngase en contacto con el Autor o el Propietario del Documento.

Las modificaciones de este documento se resumen en la siguiente tabla en orden cronológico inverso (primero la última versión).

Revisión	Fecha	Creada por	Breve descripción de los cambios
0.0	07/10/25	Sergio Zaera Mata	Preparación ToC
0.1	03/11/25	Sergio Queraltó, Jaime Castro	Contribuciones técnicas iniciales
0.2	28/11/25	UTE ForensIA (Todos)	Revisión & Contribuciones adicionales
1.0	05/12/25	Sergio Zaera Mata	1º Borrador
1.1	16/01/26	UTE ForensIA (Todos)	Contribuciones técnicas
1.2	21/01/26	Sergio Queraltó, Jaime Castro	Revisión & Consolidación
2.0	26/01/26	Sergio Zaera Mata	2º Borrador

Cofinanciado por la Unión Europea
Fondos Europeos

ADVERTENCIA DE CONFIDENCIALIDAD Y RESPONSABILIDAD LEGAL

Este documento contiene información confidencial y secretos empresariales propiedad de la UTE FORENSIA THOT, protegidos por la Ley 1/2019 de Secretos Empresariales, el artículo 13 de la Ley de Contratos del Sector Público (LCSP) y la Directiva (UE) 2016/943 sobre protección de know-how.

Se entrega exclusivamente para la finalidad prevista en el procedimiento administrativo o contractual.

Queda terminantemente prohibida su reproducción, divulgación, cesión o uso por terceros sin autorización expresa y por escrito.

El incumplimiento de estas obligaciones puede constituir:

- Infracción contractual, con las consecuencias previstas en la LCSP.
- Responsabilidad civil y penal, conforme a la Ley 1/2019 y al Código Penal (arts. 278 y ss.).
- Acciones judiciales inmediatas, incluyendo reclamación de daños y perjuicios y medidas cautelares.

Si usted no es el destinatario autorizado, debe comunicarlo de inmediato y proceder a la eliminación del documento. Cualquier uso indebido será perseguido con el máximo rigor legal".

TABLA DE CONTENIDOS

Cofinanciado por la Unión Europea
Fondos Europeos

1. INTRODUCCIÓN

1.1. Resumen Ejecutivo

El entregable *F1.3.3 Plan de Pruebas de Interoperabilidad* establece el marco metodológico y operativo para validar la correcta interacción entre la plataforma THOT, los prototipos desarrollados por el Lote 2 y los sistemas tecnológicos de la Policía Nacional. Su propósito es garantizar que los distintos componentes, desarrollados por contratistas diferentes y operando en contextos heterogéneos, puedan intercambiar información de manera segura, coherente y conforme al protocolo definido en el *Acuerdo de Interoperabilidad*. Este plan complementa al *F1.1.4 Plan de Pruebas*, centrándose específicamente en los aspectos de integración técnica, semántica y de flujo entre sistemas.

El documento define el alcance de las pruebas, los elementos implicados, los actores que intervienen y los procedimientos para asegurar la calidad durante todo el ciclo de desarrollo. Se establece una estrategia basada en metodologías ágiles, combinando validación continua mediante sandboxes, pruebas de integración, pruebas funcionales end-to-end e hitos formales de interoperabilidad con implementaciones reales del Lote 2 y con sistemas policiales existentes. Asimismo, se incorporan técnicas avanzadas de verificación como contract testing, pruebas de resiliencia en red degradada, validación criptográfica, análisis de seguridad y pruebas específicas de cadena de custodia digital.

Finalmente, el plan describe los mecanismos de comunicación, las métricas de cobertura y calidad, el uso de entornos controlados de pruebas, los entregables previstos y el cronograma de ejecución. Con este enfoque estructurado, progresivo y alineado con los requisitos del proyecto THOT, se garantiza que la interoperabilidad se aborde de forma temprana, planificada y medible, minimizando riesgos y asegurando que la solución final opere de manera robusta, segura y completamente integrada en el ecosistema forense de la Policía Científica.

1.2. Propósito del documento

El propósito central del documento F1.3.3 Plan de Pruebas de Interoperabilidad (PPI) es establecer el marco formal y metodológico que regirá la verificación y validación de la integración técnica y funcional entre los sistemas desarrollados por el Lote 2 (Interfaces operativos y equipos y sistemas para la captación y tratamiento de datos en la escena) y la plataforma THOT.

Este Plan es fundamental para garantizar que las implementaciones de los lotes 2, aunque desarrolladas por separado, operan de manera coherente, coordinada e integrada con THOT, asegurando así la eficacia global de la solución.

1.3. Alcance

El objetivo de este documento es proporcionar la información y el marco necesarios para planificar y ejecutar todos los procesos de prueba requeridos para la validación de la interoperabilidad de la plataforma THOT.

Cofinanciado por la Unión Europea
Fondos Europeos

1.4. Referencias

Los siguientes documentos constituyen la base de referencia para la elaboración y ejecución del presente Plan de Pruebas de Interoperabilidad. Incluyen tanto la documentación de diseño como el Plan de Pruebas y el Acuerdo de Interoperabilidad:

- F1.1.1. Documento de Prestaciones Funcionales y Técnicas: define los requisitos funcionales y técnicos que deben cumplir los sistemas y equipos involucrados en la interoperabilidad.
- F1.1.2. Documento de Arquitectura del Sistema: describe la arquitectura general del sistema THOT, especificando los módulos funcionales, sus interacciones, las interfaces, los protocolos de comunicación y los estándares.
- F1.1.3. Modelo de Datos: define las entidades y relaciones principales del dominio de THOT.
- F1.1.4 Plan de Pruebas: documento que describe la estrategia general de pruebas, los tipos de pruebas a realizar y los criterios de aceptación.
- F1.3.1 Acuerdo de Interoperabilidad: documento que constituye el protocolo de interoperabilidad, estableciendo los compromisos, responsabilidades y condiciones acordadas entre las partes para garantizar la correcta interacción entre sistemas. Este protocolo describe los procedimientos, estándares y mecanismos que regulan el intercambio de información y la operación conjunta.

1.5. Glosario

Término/Acrónimo	Definición
API	Interfaz de Programación de Aplicaciones que permite la comunicación entre componentes o sistemas.
CI/CD	Procesos automatizados de integración y despliegue continuo del software.
Endpoint	Punto de acceso expuesto por una API para realizar operaciones.
Hash	Valor criptográfico usado para verificar integridad de ficheros o vestigios.
mTLS	Autenticación mutua mediante certificados para cliente y servidor.
Sandbox	Entorno aislado utilizado para pruebas controladas de integración o interoperabilidad.
TUS Protocol	Protocolo robusto para cargas de ficheros con reanudación.
WebRTC	Tecnología para comunicaciones multimedia en tiempo real.

2. COMPLETITUD Y COBERTURA DEL PLAN DE PRUEBAS

A continuación, se detallan los aspectos más relevantes del contexto al que se aplicará el plan de pruebas de interoperabilidad, incluyendo a qué elementos aplica, dependencias externas al proyecto, el alcance previsto para las mismas y el detalle de actores interesados y su papel en el desarrollo y aplicación del plan de pruebas de interoperabilidad.

2.1. Proyecto de pruebas

El presente Plan de Pruebas de Interoperabilidad aplicará a los interfaces que permiten al sistema THOT interactuar con elementos externos. Este plan de pruebas de interoperabilidad se complementa con el F1.1.4. Plan de Pruebas, enfocado principalmente a la validación del cumplimiento de los requisitos, así como del correcto funcionamiento de la solución y sus componentes.

Los documentos que detallan el alcance del sistema THOT son los siguientes:

- F1.1.1. Documento de prestaciones técnicas y funcionales
- F1.1.2. Documento de arquitectura del sistema
- F1.1.3. Documento de modelo de datos

Asimismo, el siguiente entregable resulta de especial relevancia para el Plan de Pruebas de Interoperabilidad, ya que formaliza el interfaz que deben implementar los lotes 1 y 2 para interactuar.

- F1.3.1. Acuerdo de Interoperabilidad

2.2. Elementos de prueba

Los elementos de prueba comprenden los componentes que integran la solución integral THOT. La arquitectura del sistema, basada en el paradigma de microservicios, propone un modelo en el que componentes con funcionalidades específicas se orquestan e interconectan para proporcionar, de manera conjunta, un servicio de alto valor destinado a la Policía Científica.

El entregable F1.1.2, Documento de Arquitectura del Sistema, describe detalladamente el diseño de dicha solución, estructurando los microservicios en categorías funcionales (servicios). Estas categorías constituyen el eje sobre el cual se articula tanto el desarrollo de la solución como la planificación de las actividades de prueba:

- Servicio Espacio de Datos
- Servicio de Procesamiento de Datos
- Servicio de Inteligencia Artificial
- Servicios de Coordinación y Gestión
- Servicio de Alertas
- Servicio de Cadena de Custodia
- Servicio de Comunicaciones

El Plan de Pruebas de Interoperabilidad, por su naturaleza, se centrará principalmente en el Servicio de Comunicaciones y en el Servicio de Procesamiento de Datos, dado que ambos son responsables de implementar y coordinar la interacción con servicios externos a la plataforma. Asimismo, el alcance del Plan incluye el resto de servicios, garantizando que la entrada y salida de información se realicen de manera coherente con el estado global del sistema y generen el impacto previsto.

2.3. Alcance de las pruebas

El alcance de pruebas para el sistema THOT se enfoca específicamente en la interoperabilidad con sistemas externos, tales como el lote 2 y otros sistemas ya existentes en Policía Científica. Este plan cubre la validación del intercambio de información, el cumplimiento de protocolos y formatos de datos comunes, así como la correcta gestión de las transiciones entre estados al interactuar con estos sistemas externos. Se incluyen pruebas que aseguren que el sistema THOT puede comunicarse eficazmente, intercambiar datos y coordinar procesos con las plataformas externas, respetando las interfaces y contratos establecidos.

Se abarca la interoperabilidad técnica y semántica con los sistemas externos, asegurando que los datos intercambiados no solo sean compatibles en formato sino también interpretables de manera coherente por todas las partes implicadas. Además, se verificará que las transiciones de estado en el flujo de trabajo forense sean consistentes y mantengan la integridad y trazabilidad de la información a lo largo del proceso colaborativo entre sistemas.

Quedan fuera del alcance otras pruebas no relacionadas con la interoperabilidad directa, como rendimiento o usabilidad, quedando estas cubiertas por el entregable F1.1.4. Plan de Pruebas. El foco principal del presente Plan de Pruebas de Interoperabilidad es asegurar la integración funcional y la continuidad del flujo de información entre THOT y los sistemas externos, garantizando la interoperabilidad a nivel técnico, semántico y de transición de estados para cumplir con los requisitos del Reto Forense.

Cofinanciado por la Unión Europea
Fondos Europeos

2.4. Interesados

El plan de pruebas comprende el ciclo de desarrollo y entrega de los desarrollos de manera integral. La siguiente tabla detalla los diferentes actores y su papel en el desarrollo de las pruebas. Los interesados (stakeholders) incluyen tanto al personal interno del proyecto como a representantes externos. Cada uno contribuye de forma distinta al aseguramiento de la calidad del producto mediante la planificación, revisión, aprobación o ejecución de las pruebas. En este caso, es especialmente relevante la implicación de las empresas encargadas de los desarrollos del lote 2, dado que su participación resulta clave para garantizar la coherencia técnica y la validación completa de las funcionalidades entregadas. Además, el Departamento de Informática de la Policía Nacional juega un papel fundamental, ya que debe proporcionar información técnica y acceso a sistemas o entornos sandbox que faciliten la integración con los sistemas ya existentes, asegurando así una compatibilidad y operatividad óptimas entre los nuevos desarrollos y la infraestructura policial vigente.

Rol	Organización	Responsabilidades principales	Nivel de implicación	Frecuencia de interacción
Responsable de Pruebas	HI IBERIA	Planificar, coordinar y supervisar todas las actividades de prueba.	Alta	Diaria
Equipo de Testing	HI IBERIA, ETRA, HERTA, HARDLINK, UPV	Diseñar, ejecutar y documentar los casos de prueba.	Alta	Diaria
Desarrolladores	HI IBERIA, ETRA, HERTA, UPV	Atender incidencias, corregir defectos y revisar resultados de pruebas.	Media	Diaria
Gestor de Proyecto	HI IBERIA, ETRA, HERTA, HARDLINK, UPV	Asegurar recursos, aprobar el plan de pruebas y gestionar riesgos.	Alta	Semanal
Responsable de Seguridad	HARDLINK	Supervisar pruebas relacionadas con seguridad y cumplimiento normativo.	Media	Según planificación
Responsables Lote 2	Empresas desarrolladoras de los prototipos de Lote 2	Garantizar la coherencia técnica, validar funcionalidades entregadas y colaborar en pruebas de integración.	Alta	Según planificación

Dep. Informática Policía Nacional	Policía Nacional	Proporcionar información técnica, acceso a sistemas y entornos sandbox para integración con infraestructura actual.	Media	Según planificación
Cliente	Policía Científica	Aprobar los resultados de aceptación y validar la adecuación al negocio.	Baja	Mensual (tras cada entrega)
Auditor Externo	CDTI	Revisar entregables para cumplimiento de contrato.	Baja	Según planificación

3. ADECUACIÓN A LOS REQUISITOS DE INTEROPERABILIDAD DEFINIDOS EN EL DAI

La presente sección resume el enfoque general del Plan de Pruebas de Interoperabilidad, estableciendo el marco necesario para validar la interacción entre la plataforma THOT y los componentes externos asociados. El plan se ajusta a la metodología ágil aplicada en el desarrollo, organizando las pruebas en torno a las épicas e historias de usuario definidas, lo que permite una verificación gradual y alineada con la evolución funcional del sistema.

Los requisitos de interoperabilidad recogidos en el pliego técnico se integran directamente en el diseño del Acuerdo de Interoperabilidad; por ello, su validación equivale a la validación efectiva de dichos requisitos. De este modo, la sección ofrece una visión clara del alcance, los elementos sometidos a prueba y los actores involucrados, garantizando que la interoperabilidad se evalúe de forma estructurada, coherente y en consonancia con los objetivos técnicos y operativos del proyecto.

Épicas

Épica	Paquete(s) de trabajo	Casos de uso vinculados	Objetivo de pruebas
EP-PT2.1 Identificación policial (reseña)	PT2.1 (T2.1.1–T2.1.3)	UC1, UC2	Validar creación de expediente, OCR, captura biométrica (NFIQ2/3), cumplimiento ISO/IEC 19794-2/5, cotejos 1:1 y 1:N (ABIS/AFIS, PERSONAS), alertas y judicialización.
EP-PT2.2A Inspección Técnico-Policial (ITP)	PT2.2 (T2.2.1–T2.2.4)	UC3	Verificar fijación multimodal de la escena, trazabilidad/ hashes, clasificación de vestigios (ISO 21043), teleasistencia CECOR, plan de remisión y seguimiento a laboratorio.
EP-PT2.2B Actuación en Emergencias (SVM)	PT2.2 (T2.2.1–T2.2.4)	UC4	Gestión integral en escenarios de víctimas múltiples: fijación multimodal, necroidentificación lofoscópica, etiquetado AM/PM, interoperabilidad internacional, trazabilidad completa bajo condiciones extremas.
EP-PT2.3A Ciclo de Inteligencia y Cadena de Custodia	PT2.3 (T2.3.1–T2.3.10)	UC5, UC7	Probar espacio de datos, gestión y explotación, ledger/cadena de custodia, distribución de tareas, alertas, dashboards, correlación automática en base a modus operandi y patrones delictivos.
EP-PT2.3B Gestión de Inventario,	PT2.3 (T2.3.1–T2.3.10)	UC8	Gestión de inventarios y recursos (ERP), planificación y ejecución de formación, aseguramiento de calidad

Cofinanciado por la Unión Europea
Fondos Europeos

Formación y Calidad			con dashboards y microservicio IA para evaluación automática.
EP-PT2.4 Preparación Fase III	PT2.4 (T2.4.1–T2.4.4)	Transversal	Pruebas preliminares de escalabilidad, validación de prototipos, sostenibilidad y mantenimiento.
EP-PT2.5 Interoperabilidad	PT2.5 (T2.5.1–T2.5.3)	UC6	Validar integraciones, sincronización offline, contratos de API, interoperabilidad con ABIS/CODIS/IBIS/PRÜM/EURODAC, red degradada.
EP-PT4 Ciberseguridad y Continuidad	PT4 (T4.2–T4.5)	Transversal	Pentesting, análisis de vulnerabilidades, alineación con ENS Alto/ISO 27001, restauración de backups, continuidad y recuperación ante desastres (Recovery Time Objective/Recovery Point Objective).

Historias de usuario / Escenarios de prueba

Épica	ID Historia	Título	Descripción
EP-PT2.1	HU-PT2.1-01	Recepción del formulario digitalizado	Recepción desde los equipos de Lote 2 el formulario digitalizado y sus metadatos para integrarlo en el expediente verificando formato y estructura conforme al protocolo.
EP-PT2.1	HU-PT2.1-02	Publicación del evento nueva reseña	Publicación de un evento estandarizado de nueva reseña para que sistemas externos lo consuman mediante el modelo push.
EP-PT2.1	HU-PT2.1-03	Consumo de captura lofoscópica	Recepción desde Lote 2 impresiones lofoscópicas normalizadas (ISO/IEC 19794-2) verificando su correcta subida y vinculación a expediente.
EP-PT2.1	HU-PT2.1-04	Sincronización de fotografías biométricas	Recepción de imágenes biométricas normalizadas (ICAO/ISO 19794-5) y registro para su uso en cotejos.
EP-PT2.1	HU-PT2.1-05	Validación de cotejo externo 1:N	Envío y recepción de resultados de cotejos con bases externas (ABIS, PERSONAS) verificando su estructura semántica y firma.
EP-PT2.1	HU-PT2.1-06	Gestión de desconexión temporal	Validación de cambios enviados tras periodo offline de Lote 2, garantizando idempotencia.

EP-PT2.1	HU-PT2.1-07	Judicialización interoperable	Remisión del paquete documental firmado y estructurado para su integración en sistemas externos.
EP-PT2.2A	HU-PT2.2A-01	Ingesta de fijación multimodal	Recepción de imágenes, vídeo, planos y 3D desde Lote 2 garantizando trazabilidad, hashes y metadatos auditables.
EP-PT2.2A	HU-PT2.2A-02	Registro interoperable de vestigios	Recepción de creaciones de vestigios conforme a ISO 21043 desde lote 2 y registro en la cadena de custodia inicial.
EP-PT2.2A	HU-PT2.2A-03	Actualización de vestigios en campo	Recepción de actualizaciones de vestigios (PATCH/PUT) desde lote 2, verificando coherencia semántica y sincronización.
EP-PT2.2A	HU-PT2.2A-04	Solicitud remota de teleasistencia	Establecimiento de sesiones seguras de teleasistencia con dispositivos de lote 2 mediante el canal de señalización seguro.
EP-PT2.2B	HU-PT2.2B-01	Registro AM/PM interoperable	Recepción de datos AM y PM para cotejo internacional garantizando su formato y trazabilidad.
EP-PT2.2B	HU-PT2.2B-02	Publicación del evento nueva víctima	Publicación de eventos PM para consumo de sistemas nacionales e internacionales.
EP-PT2.2B	HU-PT2.2B-03	Envío de perfiles dactilares y ADN	Envío y recepción de resultados de cotejos con sistemas AFIS/ADN/PRÜM verificando la estructura y firma.
EP-PT2.3A	HU-PT2.3A-01	Recepción de actualizaciones de cadena de custodia	Recepción de eventos sujetos a cadena de custodia desde Lote 2 garantizando firma, timestamp y coherencia secuencial.
EP-PT2.3A	HU-PT2.3A-02	Vinculación automática entre casos	Procesado de eventos externos para actualizar grafos y vínculos entre casos conforme a modelos JSON-LD.
EP-PT2.3A	HU-PT2.3A-03	Distribución de alertas	Generación y transmisión de alertas interoperables con auditoría completa.
EP-PT2.4	HU-PT2.4-01	Validación inicial de escalabilidad de integración	Ejecución de pruebas de carga sobre el interfaz de interoperabilidad verificando estabilidad y límites.
EP-PT2.5	HU-PT2.5-01	Envío de vestigios a sistemas internacionales	Envío de evidencias normalizadas a sistemas internacionales garantizando estructura, trazabilidad y firma.
EP-PT2.5	HU-PT2.5-02	Sincronización offline completa	Validación de la operación y sincronización de datos de Lote 2 tras periodo de

			funcionamiento offline, preservando orden e integridad.
EP-PT2.5	HU-PT2.5-03	Manejo de errores interoperables	Validación de la correcta interpretación de errores 2xxx/3xxx por parte de los clientes.
EP-PT4	HU-PT4-01	Validación de mTLS + OIDC	Validación de certificados y tokens OIDC en todas las peticiones originadas por Lote 2, asegurando trazabilidad absoluta.
EP-PT4	HU-PT4-02	Firma digital de datos	Validación de firma digital ECDSA y sello de tiempo verificable en todos los datos incorporados desde Lote 2.
EP-PT4	HU-PT4-03	Validación en red degradada	Validación del correcto funcionamiento de la interoperabilidad con Lote 2 en condiciones de latencia, pérdida de paquetes y reconexiones.

Cofinanciado por la Unión Europea
Fondos Europeos

4. COMUNICACIÓN DE LAS PRUEBAS

La comunicación entre los equipos de desarrollo, pruebas y partes interesadas se organizará conforme a los principios de transparencia y colaboración continua del marco Agile. Las pruebas de interoperabilidad se planificarán únicamente en sprints específicos, definidos como hitos dentro del cronograma del proyecto. Para ello, se ajustará la carga de trabajo de dichos sprints, garantizando espacio suficiente para la ejecución de estas pruebas.

Al inicio de cada sprint que incluya pruebas de interoperabilidad, se celebrará una reunión conjunta entre el equipo de desarrollo y el equipo de pruebas con el objetivo de:

- Revisar las historias de usuario seleccionadas.
- Acordar criterios de aceptación.
- Definir los casos de prueba iniciales y escenarios funcionales prioritarios.
- Validar la viabilidad técnica de las actividades de verificación.

Durante el ciclo de desarrollo, la coordinación se mantendrá mediante reuniones breves de seguimiento y el uso de herramientas de gestión compartidas, que permitirán al equipo de pruebas mostrar el avance, los defectos detectados y el estado de corrección. La comunicación informal se complementará con procedimientos formalizados (ClickUp), donde se registrarán incidentes y tareas derivadas de la ejecución de pruebas.

Al cierre de cada sprint con pruebas de interoperabilidad, el equipo de pruebas generará un informe resumido específico que incluirá:

- Número total de pruebas ejecutadas, organizadas por tipo.
- Porcentaje de pruebas superadas y fallidas.
- Evolución del porcentaje de cobertura de métodos de interfaz.
- Número y criticidad de defectos abiertos y cerrados.
- Tendencias respecto al informe anterior.

Para optimizar el tiempo de elaboración, se prevé que este informe sea generado de manera semiautomática mediante integraciones con herramientas de CI/CD y sistemas de seguimiento de pruebas.

Los defectos no resueltos se reintroducirán en el ciclo de desarrollo, etiquetados conforme a su prioridad y severidad, y programados para validación en la siguiente prueba de interoperabilidad. Además, se habilitará un canal formal para el cliente, mediante formulario de reporte de defectos, que garantizará la trazabilidad desde la notificación hasta la resolución.

Los informes generados en cada sprint con pruebas se consolidarán en los entregables *F2.3.1. Informe de pruebas de interoperabilidad (fase 2)* y *F3.3.1. Informe de pruebas de interoperabilidad finales (fase 3)*.

Estos documentos incluirán todos los informes parciales y constituirán la base para justificar el nivel de calidad alcanzado por el sistema al finalizar cada fase.

5. Registro de Riesgos (Risk Register)

El desarrollo de THOT seguirá un enfoque *security-by-design*. En este marco, se han identificado los riesgos de interoperabilidad sobre los que se realizará seguimiento en el diseño de las pruebas de interoperabilidad de THOT.

ID	Riesgo asociado a pruebas	Descripción	Prob.	Impacto	Mitigación
R1	Retrasos en la disponibilidad de accesos/aprobaciones por parte de otros contratistas.	La liberación de accesos o aprobaciones del lote 2 se retrasa, impidiendo iniciar pruebas según el planning	Media	Alta	Alinear cronogramas con contratistas de lote 2, realizar reuniones de coordinación, solicitar visibilidad anticipada de hitos críticos y disponer de escenarios
R2	Dependencias técnicas no resueltas entre lotes	Interfaces técnicas incompletas o mal definidas entre lotes que bloquean o invalidan pruebas planificadas.	Media	Alta	Revisar interfaces tempranamente, acordar responsables por cada punto de interfaz, establecer mecanismo formal de comunicación para su resolución (versionado del acuerdo de Interoperabilidad).
RC 1	Suplantación de sistemas externos	Riesgo de que un sistema no autorizado se haga pasar por un componente legítimo del Lote 2 o de la infraestructura de la Policía Nacional para enviar o recibir información.	Baja	Alta	Establecer autenticación mutua estricta (certificados, MTLS), listas blancas de endpoints autorizados, validación de claves públicas, y monitorización continua del tráfico para detectar anomalías.
RC 2	Ataques Man-in-the-Middle en canales de interoperabilidad	Intercepción y posible modificación de los mensajes intercambiados entre THOT y los sistemas externos si los canales no están	Baja	Alta	Forzar cifrado TLS 1.3, aplicar firma digital de mensajes, activar validación estricta de certificados, y usar canales dedicados o túneles VPN con controles reforzados.

		correctamente cifrados y autenticados.			
RC 3	Pérdida de integridad en la cadena de custodia digital	Inconsistencias entre los registros de THOT y los sistemas externos respecto a identificadores de evidencias, valores de hash o estados, que puedan comprometer la validez probatoria de la información.	Baja	Alta	Implementar doble verificación de hashes, reconciliación automatizada entre lotes, auditorías periódicas de integridad y almacenamiento inmutable de evidencias.
RC 4	Fuga de información sensible en entornos de prueba	Utilización inadecuada de datos reales o pseudonimizados en el entorno de staging, con acceso no controlado por parte de terceros o de perfiles que no requieren conocer dicha información.	Baja	Alta	Garantizar anonimización/pseudonimización total, limitar accesos por RBAC, usar entornos aislados, revisar logs de acceso y aplicar borrado seguro tras las pruebas.
RC 5	Errores de mapeo semántico entre sistemas	Interpretación incorrecta de campos o códigos entre THOT y los sistemas externos, que genere decisiones erróneas o pérdida de contexto forense relevante.	Baja	Media	Alinear diccionarios de datos, validar esquemas de intercambio, realizar pruebas de compatibilidad tempranas, y documentar exhaustivamente los mapeos entre sistemas.
RC 6	Configuraciones inseguras en el entorno de pruebas de interoperabilidad	Falta de medidas de seguridad en el entorno openstack/Kubernetes o en los sandboxes, que	Baja	Alta	Aplicar endurecimiento del clúster, revisar configuraciones por CIS Benchmark, usar escáneres de seguridad, activar políticas de red

		permitan accesos no autorizados, escaladas de privilegios o manipulación de servicios.			(NetworkPolicies) y limitar permisos con PodSecurity Standards.

6. DEFINICIÓN DE ESCENARIOS DE PRUEBA, CASOS DE USO, DATOS DE PRUEBA, CRITERIOS DE ACEPTACIÓN Y LAS MÉTRICAS DE ÉXITO

La estrategia de pruebas del proyecto THOT se alineará con la metodología Agile, manteniendo el enfoque en la calidad continua de los entregables de cada sprint. En el caso de las pruebas de interoperabilidad, estas se dividirán en dos bloques. De manera continua, integrada con los mecanismos de CI/CD, se realizarán baterías de pruebas contra sandbox de lote 2 (interacciones simuladas). Las pruebas contra implementaciones reales de contratistas de lote 2 se planifican de forma puntual, estableciendo hitos específicos dentro del calendario del proyecto. Dichos hitos permitirán validar la correcta interacción entre sistemas y garantizar la conformidad con el protocolo definido.

Antes de cada hito de interoperabilidad, se considera prerrequisito que los componentes individuales hayan superado sus pruebas unitarias y de integración internas, responsabilidad del equipo de desarrollo y sujeto al Plan de Pruebas. El presente plan no detalla dichas pruebas, ya que su objetivo principal es la validación de la interoperabilidad entre sistemas.

El equipo de desarrollo y el equipo de pruebas colaborarán estrechamente desde la planificación, definiendo criterios de aceptación claros y casos de prueba derivados de las historias de usuario y de los escenarios de interoperabilidad previstos para cada hito.

Las pruebas incluidas en este plan abarcarán principalmente:

- Pruebas de integración entre sistemas participantes.
- Pruebas funcionales para validar flujos completos.
- Pruebas de aceptación según criterios definidos.
- Pruebas específicas de interoperabilidad, orientadas a verificar la correcta comunicación y cumplimiento del protocolo.

Asimismo, la estrategia incluye la integración de métricas de calidad (como cobertura de pruebas, número de defectos abiertos y tiempo medio de resolución) para ofrecer una visión objetiva del estado del producto en cada iteración y en cada hito de interoperabilidad.

6.1. Subprocesos de pruebas

6.1.1. Pruebas de integración

Las pruebas de integración se realizarán con el objetivo de confirmar que la plataforma THOT interactúa correctamente con los sistemas externos contemplados en su diseño. En esta fase se busca garantizar que las interfaces técnicas, los protocolos de comunicación y los mecanismos de intercambio de información funcionan de manera consistente y fiable en un entorno controlado.

Durante estas pruebas se validará que los datos se transmiten en el formato esperado, que las respuestas se gestionan adecuadamente y que no se producen errores en la comunicación directa. Además, se simularán condiciones adversas, como tiempos de respuesta variables o interrupciones en la conexión, para comprobar la capacidad del sistema de mantener una integración robusta y tolerante a fallos.

6.1.2. Pruebas funcionales

Estas pruebas tienen como objetivo confirmar que el sistema mantiene su comportamiento funcional completo cuando interactúa con sistemas externos en escenarios realistas. No se trata únicamente de verificar que cada función aislada opera correctamente, sino de asegurar que los procesos end-to-end respetan las reglas de negocio y producen resultados coherentes cuando la información o los eventos provienen de otros sistemas.

Estas pruebas permitirán validar que la lógica interna de la plataforma THOT no se ve comprometida por la interoperabilidad y que las operaciones que dependen de datos externos se ejecutan de forma correcta y fiable, garantizando que la funcionalidad prevista se mantiene intacta en un entorno donde la interacción con terceros es parte del flujo operativo.

6.1.3. Pruebas de interoperabilidad

Las pruebas de interoperabilidad representan el núcleo del plan y se centran en asegurar que sistemas independientes, desarrollados por diferentes organizaciones, interactúan correctamente en condiciones reales y siguiendo el protocolo acordado. A diferencia de las pruebas de integración, aquí no basta con validar la comunicación técnica: es fundamental comprobar que todos los sistemas interpretan los mensajes de forma coherente, respetan la secuencia de operaciones y gestionan los errores conforme a lo establecido.

Estas pruebas se llevarán a cabo en un entorno que refleje la realidad del ecosistema, evaluando la robustez del intercambio de información, la tolerancia ante fallos y la capacidad de recuperación frente a incidentes. El objetivo final es garantizar que la interoperabilidad no solo es posible, sino también fiable y alineada con los objetivos del proyecto.

Conforme los sistemas reales del Lote 2 estén disponibles y operativos, se repetirá el conjunto de pruebas de interoperabilidad empleando dichos sistemas, con el fin de validar la interoperabilidad efectiva en condiciones reales y certificar la conformidad con el protocolo. Las pruebas realizadas sobre el sandbox tienen carácter preparatorio y no sustituyen las pruebas sobre los sistemas definitivos.

6.1.4. Pruebas de Ciberseguridad

Las pruebas de ciberseguridad constituyen un componente transversal del Plan de Pruebas de Interoperabilidad y tienen como objetivo verificar que los intercambios de información entre THOT, los sistemas del Lote 2 y los sistemas TIC de la Policía Nacional se realizan dentro de un entorno seguro. Estas pruebas garantizan el cumplimiento de los principios de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. Su finalidad no se limita a comprobar la solidez técnica de los mecanismos de protección, sino también a asegurar que dichos mecanismos mantienen su eficacia cuando se integran en los flujos operativos reales del ecosistema forense, especialmente en aquellos relacionados con evidencias, vestigios y metadatos de carácter probatorio.

Asimismo, las pruebas de ciberseguridad se orientan a validar el comportamiento seguro del sistema cuando las integraciones y los flujos funcionales operan en condiciones reales o adversas, evaluando la capacidad de la plataforma para resistir ataques, fallos, manipulaciones o usos indebidos.

6.2. Entregables de prueba

Los entregables derivados del Plan de Pruebas de Interoperabilidad tienen como objetivo documentar de manera sistemática los resultados obtenidos en las actividades de verificación

y validación, asegurando la trazabilidad con los requisitos de interoperabilidad definidos en en el pliego técnico del proyecto y contemplados en el F1.3.1 Acuerdo de Interoperabilidad. Estos entregables se generarán de forma iterativa, alineados con la planificación del proyecto y los sprints definidos en la metodología ágil., y supondrán la base para la generación del entregable de fase 2 *F2.3.1 Informe de pruebas de interoperabilidad* y del entregable de fase 3 *F3.3.1 Informe de pruebas de interoperabilidad finales*.

Todos los entregables contendrán anexos generados automáticamente desde las herramientas de CI/CD utilizadas en el proyecto. Los informes por sprint se emitirán cada cuatro semanas, mientras que los informes específicos (interoperabilidad con lotes 2 de otros contratistas, ciberseguridad) se elaborarán en los hitos definidos en el cronograma.

Cada entregable incluirá referencias a los requisitos de interoperabilidad, los casos de prueba definidos para el sprint y los criterios de aceptación correspondientes, asegurando la coherencia y la cobertura completa del alcance previsto.

6.2.1. *Informes por sprint*

Al finalizar cada sprint se elaborará un informe que recoja el estado de las pruebas ejecutadas. Este informe incluirá el número total de pruebas realizadas, clasificadas por componentes involucrados, tipo, el porcentaje de pruebas superadas y fallidas, la evolución de la cobertura de código, así como el número y criticidad de los defectos abiertos y cerrados. Se incorporarán tendencias respecto al sprint anterior para facilitar la toma de decisiones.

6.2.2. *Informes de interoperabilidad*

Se redactarán informes específicos destinados a verificar la correcta integración de THOT con las distintas implementaciones del lote 2 desarrolladas por otros contratistas. Dichos informes recogerán los resultados de las pruebas de interoperabilidad realizadas conjuntamente con los equipos responsables de cada implementación del lote 2, basándose en pruebas previamente validadas sobre el entorno sandbox. Toda la información reflejada en estos informes se sustentará en datos recopilados de forma sistemática.

6.2.3. *Informes de pruebas de ciberseguridad*

Los informes de pruebas de ciberseguridad recogerán los resultados de las evaluaciones realizadas sobre los mecanismos de autenticación, autorización, cifrado y protección de los canales de comunicación entre THOT y los sistemas externos. Incluirán evidencias sobre la integridad y trazabilidad de los mensajes, la gestión de errores y la respuesta ante mensajes malformados o ataques de repetición, así como los resultados de pruebas de perturbación, inyección de fallos y simulación de condiciones adversas de red. Cada informe resumirá las incidencias detectadas, su criticidad, el impacto potencial sobre la cadena de custodia digital y las acciones de mitigación propuestas, proporcionando una visión clara del nivel de seguridad alcanzado durante la interoperabilidad.

6.3. Técnicas de diseño de pruebas

El diseño de las pruebas de interoperabilidad se apoya en un conjunto de técnicas progresivas que permiten validar tanto la conformidad estructural del protocolo como el comportamiento secuencial, transaccional y seguro de los intercambios entre la plataforma THOT, en su papel de servidor del lote 1, y los sistemas del lote 2 o sistemas externos de la Policía Científica. Estas técnicas cubren desde el análisis estático de las definiciones del Acuerdo de

Interoperabilidad hasta la validación dinámica de flujos completos en condiciones adversas, incluyendo aspectos de ciberseguridad y resiliencia de red.

En primer lugar, se aplicarán técnicas basadas en especificación orientadas a garantizar que las estructuras de datos definidas en el protocolo se implementan correctamente. Esto incluye la validación detallada de esquemas JSON y JSON-LD, la verificación de cardinalidades, formatos, tipos y requisitos de auditoría, así como la comprobación de que los mecanismos de transporte, autenticación y trazabilidad establecidos por el *Acuerdo de Interoperabilidad* se cumplen de manera estricta. Sobre esta base se aplicarán técnicas de partición de equivalencias y análisis de valores límite, que permiten definir conjuntos representativos de entradas y explorar los límites funcionales del sistema, especialmente relevantes en parámetros como paginación, filtros, tamaños máximos de ficheros o variaciones en los metadatos de auditoría.

Junto con ello, se incorporan pruebas de contrato (contract testing), fundamentales en un contexto multiproveedor donde THOT actúa como servidor y garante del protocolo. Estas pruebas permitirán validar la compatibilidad semántica y estructural entre las distintas implementaciones del lote 2, asegurando que todas interpretan de forma coherente los códigos de estado, los mecanismos de actualización de recursos, el modelo de idempotencia o la gestión de conflictos basada en marcas temporales. Esta técnica se utilizará tanto sobre sandboxes como sobre implementaciones reales para garantizar la estabilidad del ecosistema.

Paralelamente se emplean técnicas de prueba negativa e inyección controlada de fallos, destinadas a demostrar la robustez de THOT frente a datos incorrectos, mensajes malformados, estructuras incompletas o violaciones deliberadas del contrato. Con estas técnicas se validará que el servidor rechaza adecuadamente mensajes que vulneran la estructura o la semántica del protocolo, que genera códigos de error 2xxx o 3xxx coherentes, y que mantiene la estabilidad del proceso incluso cuando recibe entradas inesperadas o maliciosas.

Como complemento, se aplicará *fuzzing* estructural y semántico sobre los distintos endpoints y colecciones del protocolo para identificar defectos en el tratamiento de datos atípicos o no declarados, garantizando que no se producen fallos de validación, excepciones no controladas o problemas en la cadena de custodia digital. Este enfoque resulta particularmente relevante en un entorno donde se intercambian datos de elevado valor probatorio y donde la integridad del formato y la semántica de los mensajes es crítica.

Dado que la interoperabilidad implica secuencias de operaciones, actualizaciones encadenadas y sincronización offline, se recurrirá a técnicas basadas en modelos, empleando máquinas de estados que permitan verificar la coherencia de las transiciones entre operaciones y estados. Estas técnicas permiten identificar transiciones inválidas, inconsistencias en la interpretación de versiones o marcas temporales, y comportamientos no previstos cuando los mensajes se repiten o se reciben en distinto orden, reproduciendo así las condiciones similares a las previstas en el entorno real.

Sobre esta base se diseñarán pruebas end to end que reproducen flujos completos de los casos de uso del proyecto, abarcando la interacción real entre dispositivos de lote 2 y THOT. Estas pruebas permitirán verificar la continuidad funcional, la correcta ejecución de la lógica de negocio y la preservación de la trazabilidad, incluyendo la generación, firma, sellado, propagación y recuperación de datos. Estas validaciones se ejecutarán tanto bajo condiciones

normales como en escenarios de red degradada, con latencia elevada, pérdidas de conectividad, cambios de IP o reconexiones abruptas, reproduciendo el funcionamiento previsto para situaciones de campo y verificando los mecanismos de reintento, sincronización diferida y consistencia secuencial.

De forma transversal, se integrarán técnicas específicas de ciberseguridad orientadas a validar que los intercambios entre lote 1 y lote 2 se producen dentro del marco de confianza definido para el ecosistema. Estas técnicas incluyen la verificación criptográfica de autenticación mutua mediante mTLS, la validación del uso correcto de tokens OIDC, la comprobación de integridad mediante firmas ECDSA y sellos de tiempo, y el análisis del comportamiento del sistema frente a intentos de ataque como modificaciones en tránsito, suplantación de plataforma, repetición de mensajes o degradación del cifrado. Se incluirán además pruebas dirigidas a garantizar la trazabilidad completa de las operaciones, verificando que todos los registros generados por THOT son íntegros, coherentes y auditables.

Finalmente, estas técnicas se complementarán con revisiones estáticas previas a la ejecución, centradas en aspectos como la revisión del acuerdo de interoperabilidad, la coherencia de los modelos de datos, la configuración del entorno Kubernetes y los requisitos de seguridad aplicados a cada componente del sistema. Este análisis previo permite identificar errores antes de la integración y asegura que el entorno en el que se ejecutan las pruebas cumple las condiciones necesarias para obtener resultados fiables.

6.4. Métricas a recopilar

Categoría	Métrica	Descripción	Umbral (sobre alcance del sprint)	Herramienta recomendada	Tipo de prueba
Cobertura de interfaz	Cobertura de endpoints del protocolo	Porcentaje de endpoints/métodos del protocolo con casos ejecutados (positivos, negativos y de error)	>=90% (>=95% críticos)	Postman; CI/CD	Integración / Interoperabilidad
Cobertura de contrato	Conformidad de contratos	Interacciones que cumplen el contrato de interoperabilidad sin desviaciones estructurales ni semánticas	>=95% (100% críticos)	Pact	Interoperabilidad
Éxito End-to-End	Tasa de éxito de flujos E2E	Porcentaje de flujos funcionales completos ejecutados	>=98%	Postman; pipelines E2E	Funcional / Interoperabilidad

		correctamente según los casos de uso			
Defectos	Densidad de defectos	Defectos abiertos por cada 100 casos ejecutados	<=5 (Sev-1=0)	ClickUp	Todas
Idempotencia	Duplicados evitados	Operaciones duplicadas para mismo identificador de petición + plataforma	0	Loki; pruebas negativas	Interoperabilidad / Ciberseguridad
Latencia	Latencia p95 API	p95 de latencias en ms	<=500ms (<=300ms críticos)	k6; Prometheus/Grafana	Rendimiento / Interoperabilidad
Estabilidad	Tasa de error 5xx	Porcentaje de respuestas 5xx respecto al total	<=0.5%	k6; Prometheus	Integración / Rendimiento
Robustez en red degradada	Correctitud bajo perturbación	Casos correctos con latencia, jitter o pérdida simulada	>=95%	Toxiproxy; Postman	Interoperabilidad / Estrés
Transferencia de archivos	Integridad de archivos	Coincidencia hash origen-destino y reanudación correcta	100%	Cliente tus; verificación hash SHA-256	Interoperabilidad / Funcional
Cadena de custodia	Consistencia de hashes	Discrepancias de hashes entre sistemas	0	Hashing; logs de auditoría	Interoperabilidad
Trazabilidad	Correlación Request-ID	Transacciones trazables en logs extremo a extremo	>=99%	Loki	Interoperabilidad / Ciberseguridad
Seguridad del canal	mTLS estricto	Conexiones establecidas con mTLS válido	100%	Monitor TLS; mitmproxy	Ciberseguridad
Protección anti-replay	Rechazo de replay	Intentos de repetición detectados y bloqueados	100%	Pruebas negativas; Loki	Ciberseguridad

Gestión de errores	Calidad de errores del protocolo	Errores conforme al catálogo estructurado (2xxx/3xxx)	>=98%	Postman	Interoperabilidad
Compatibilidad multi-L2	Aprobación cruzada multi-prototipo	Pruebas comunes aprobadas con distintas implementaciones del lote 2	100% subconjunto crítico	Postman; Pact	Interoperabilidad
Versionado	Rupturas entre versiones	Breaking changes no declarados	0	Pact	Interoperabilidad
Autenticación	Éxito OIDC + RBAC	Peticiones autenticadas/autorizadas correctamente	>=99%	Keycloak; Postman	Ciberseguridad / Interoperabilidad
Auditabilidad	Integridad de logs	Eventos firmes/inmutables disponibles	100% críticos	Loki	Ciberseguridad
Automatización	Tasa de automatización	Porcentaje de casos ejecutados automáticamente en CI/CD	>=85%	CI/CD; Postman; k6	Todas
WebRTC	Estabilidad de señalización	Sesiones con ICE/SDP completado y media estable	>=95% bajo <=2% pérdida	Tests de señalización; Toxiproxy	Interoperabilidad / Estrés

6.5. Requisitos de datos de prueba

En el marco del Plan de Pruebas de Interoperabilidad, y con el objetivo de garantizar la coherencia entre actividades de validación y minimizar el esfuerzo de preparación de entornos y datasets, se emplearán los mismos datos de prueba definidos y generados conforme al *F1.1.4. Plan de Pruebas*. Dichos datos serán elaborados considerando la representatividad funcional, la anonimización necesaria y la reutilización en los diferentes entornos del proyecto, por lo que resultan igualmente adecuados para los escenarios de interoperabilidad previstos. En consecuencia, el presente plan no introduce nuevos conjuntos de datos específicos, sino que se apoya en los datasets establecidos en el *F1.1.4*, asegurando así consistencia, trazabilidad y continuidad en la validación entre lotes y sistemas externos.

6.6. Requisitos del entorno de pruebas

El proceso de verificación y validación de la interoperabilidad de la plataforma THOT se apoyará en un único entorno de pruebas (staging), diseñado para cubrir todas las fases del ciclo de pruebas. Este entorno permitirá reproducir con fidelidad las condiciones necesarias

para ejecutar los distintos tipos de prueba previstos: integración, funcionales y de interoperabilidad.

El entorno de pruebas se desplegará sobre la infraestructura privada instanciada por la UTE (entorno Kubernetes sobre OpenStack), aprovechando el entorno de staging aprovisionado conforme a lo descrito en el *F1.1.4. Plan de Pruebas*. Este entorno constituirá el punto central para la integración técnica entre los distintos módulos y servicios que componen la plataforma THOT, y servirá para realizar ensayos en condiciones funcionales y de carga cercanas a las de un sistema operativo, incluyendo pruebas de interoperabilidad.

Su configuración estará definida mediante ficheros de despliegue declarativos en Kubernetes, que determinarán de forma precisa las versiones de las imágenes, las variables de configuración, los recursos asignados y las dependencias entre servicios. Dichos ficheros constituirán la referencia oficial del entorno y se mantendrán bajo control de versiones, asegurando la trazabilidad de toda modificación y posibilitando la reproducción de un estado exacto del sistema en cualquier momento. Los despliegues se ejecutarán a través de procedimientos automatizados de integración y entrega continua (CI/CD).

Adicionalmente, se desarrollará un sandbox específico para el lote 2, así como tantos sandboxes de sistemas de Policía Nacional como sea necesario, en caso de que no existan. Estos entornos complementarios permitirán realizar pruebas aisladas y simulaciones controladas, asegurando la interoperabilidad y la correcta integración con los sistemas externos implicados desde las fases tempranas de desarrollo.

7. Actividades de Prueba y Estimaciones

La validación continua frente al sandbox del lote 2 será una parte fundamental del proceso de verificación a lo largo de todo el desarrollo. Su integración directa en los ciclos habituales de pruebas —tanto dentro de cada sprint como en las actividades de regresión— permitirá identificar de forma temprana cualquier desviación respecto al protocolo, incoherencia semántica o incompatibilidad técnica. Con ello se evitará la acumulación de incidencias que pudieran comprometer la calidad y la estabilidad de los hitos posteriores. Este enfoque asegura que cada incremento evolucione alineado con el *Acuerdo de Interoperabilidad*, reforzando la solidez del sistema desde las fases iniciales del proyecto.

Sobre esta base de validación continua, las pruebas de interoperabilidad con las implementaciones del lote 2 desarrolladas por otros contratistas se configurarán como hitos específicos en el cronograma. En concreto, durante la segunda mitad de la fase 2 y a lo largo de la fase 3 se realizarán pruebas cruzadas tanto con implementaciones reales de terceros como con los sandboxes de los sistemas de la Policía Científica. Esta progresión permitirá comprobar el comportamiento del ecosistema en escenarios más amplios y realistas, donde la coordinación entre proveedores resulta especialmente relevante.

La combinación de validación temprana y continua, junto con hitos formales de interoperabilidad, reducirá riesgos, permitirá anticipar incompatibilidades y garantizará que la solución final proporcione una interacción robusta, coherente y plenamente operativa en un entorno real.

Cofinanciado por la Unión Europea
Fondos Europeos

8. Dotación de Personal

El Plan de Pruebas de Interoperabilidad se llevará a cabo con el mismo equipo de pruebas definido en el documento *F1.1.4 Plan de Pruebas*, conservando su estructura, roles y responsabilidades, dado que las actividades de interoperabilidad forman parte integral de la estrategia global de validación del sistema THOT.

Este equipo, integrado por responsables de pruebas, personal de QA, especialistas en ciberseguridad y desarrolladores, asumirá igualmente las tareas específicas relacionadas con la verificación de interfaces, la validación de contratos, la ejecución de escenarios multi-lote y la gestión de los entornos compartidos.

Cofinanciado por la Unión Europea
Fondos Europeos

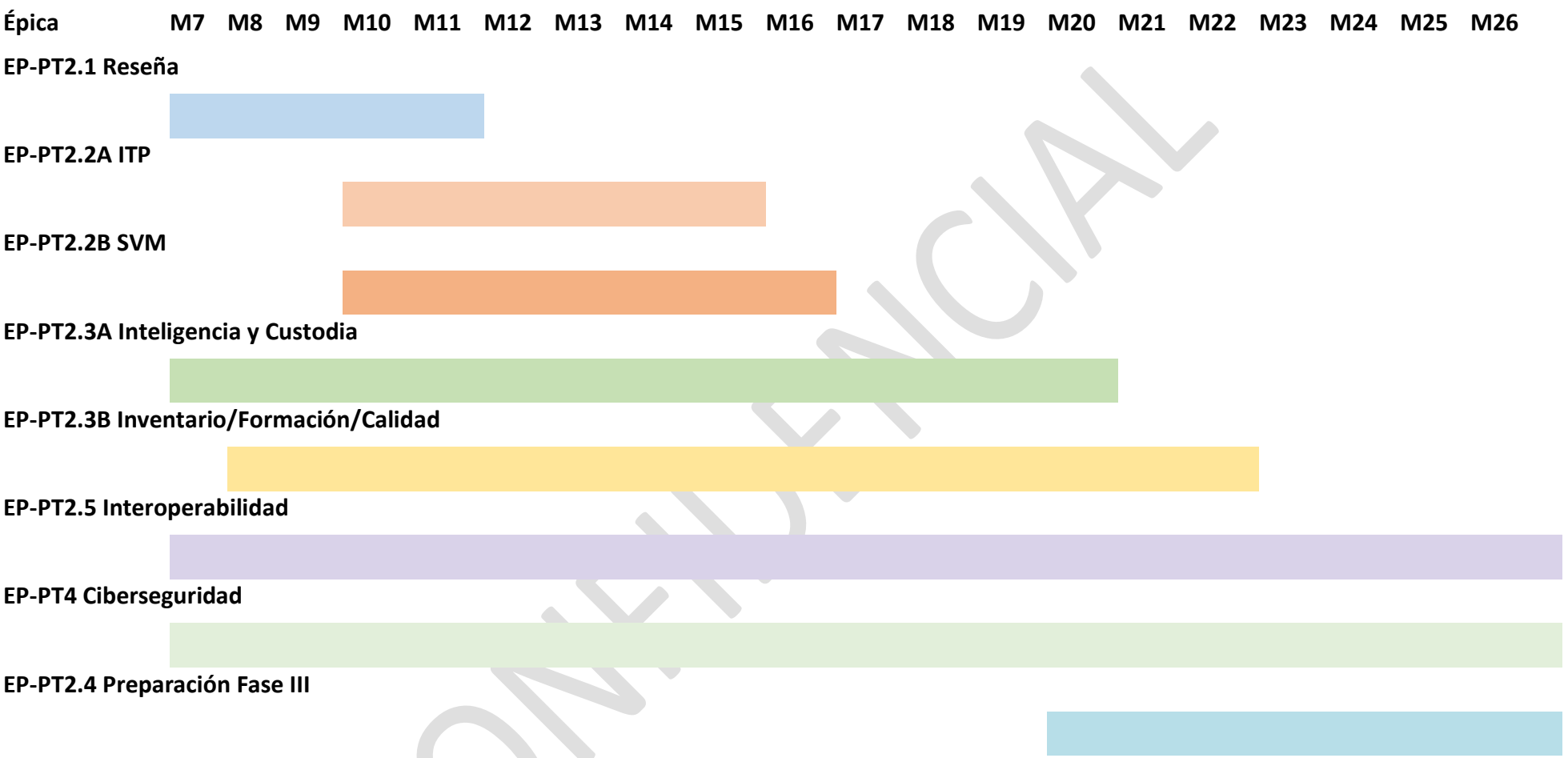
9. CRONOGRAMA

El proyecto se desarrollará bajo un enfoque ágil, organizado en sprints de cuatro semanas que permitirán una planificación iterativa e incremental, asegurando entregas funcionales y verificables en cada ciclo. La estructura se basa en épicas derivadas de los paquetes de trabajo, desglosadas en historias de usuario con criterios de aceptación para garantizar la calidad. Estas historias se distribuirán progresivamente según prioridad, complejidad y dependencias, de modo que cada sprint concluya con un incremento validado y potencialmente desplegable, favoreciendo la retroalimentación continua entre desarrollo, pruebas y Policía Científica.

Las pruebas de interoperabilidad se programarán como hitos específicos, realizándose una vez cada cuatro sprints, comenzando en el cuarto sprint. Estas pruebas se integrarán en el cronograma como actividades clave para verificar la correcta interacción entre los distintos componentes del sistema y asegurar la conformidad con los requisitos del protocolo. De este modo, se garantiza que la validación de la interoperabilidad se realice de manera planificada y alineada con el avance del desarrollo.

El presente plan de pruebas incorpora un cronograma preliminar que servirá como base para la planificación del trabajo en las fases posteriores del proyecto. Dicho cronograma se ajustará conforme al avance del proyecto y a los resultados de las revisiones de sprint. De esta manera, se mantendrá la flexibilidad necesaria para incorporar mejoras o ajustes derivados de la evaluación continua del proceso de desarrollo y de la calidad de las entregas intermedias.

Cofinanciado por la Unión Europea
Fondos Europeos



10. TECNOLOGÍAS DE SOPORTE A LAS PRUEBAS

La validación de la interoperabilidad entre la plataforma THOT, las diferentes implementaciones del Lote 2 y, los sistemas TIC de la Policía Nacional requiere un conjunto especializado de herramientas que garantice la automatización de las pruebas, la coherencia de los contratos de intercambio de información, la robustez de los flujos ante condiciones adversas, la seguridad extremo a extremo y la trazabilidad completa de todas las interacciones.

En esta sección se describen las herramientas seleccionadas para la ejecución del plan de pruebas de interoperabilidad, detallando su función, su ámbito de aplicación y su aportación al aseguramiento de la calidad en pruebas de integración, funcionales y de interoperabilidad.

Pruebas de integración

En las pruebas de integración, en las que debe verificarse el comportamiento de THOT frente a sistemas externos aún no disponibles (implementaciones del Lote 2 o sandboxes de sistemas policiales), se utilizará **Postman** como herramienta cliente para generar solicitudes controladas que reproduzcan los casos definidos en el Acuerdo de Interoperabilidad. A partir de dichas definiciones, Postman permitirá construir colecciones y entornos de prueba capaces de emitir peticiones estructuradas conforme al protocolo, incluyendo cuerpos de datos válidos, secuencias de llamadas, encabezados, códigos de error y variaciones semánticas necesarias para la validación exhaustiva del servidor THOT. Este enfoque permitirá simular escenarios completos de integración desde el punto de vista del cliente: creación y actualización de recursos, consultas, sincronización offline, validación de idempotencia, manejo de estados y verificación de errores. Todo ello se realizará de forma repetible y sin depender del despliegue real de los sistemas externos.

Además, este sandbox de pruebas se complementará con **Pact**, que se empleará para validar los contratos entre THOT (como proveedor del servicio) y cada implementación del Lote 2 (como consumidor). Pact permitirá detectar divergencias en la estructura, semántica o versionado del protocolo antes de ejecutar pruebas reales de interoperabilidad, garantizando así la coherencia de los contratos y evitando fallos en fases posteriores.

Pruebas funcionales

En el ámbito de las pruebas funcionales, cuyo propósito es validar que THOT ejecuta correctamente los flujos operativos cuando interactúa con servicios externos, se utilizarán herramientas orientadas a la ejecución de escenarios end-to-end en condiciones cercanas al uso real.

Las colecciones de **Postman** se emplearán para verificar flujos completos: desde la ingesta de evidencias y vestigios procedentes del Lote 2 hasta la publicación de eventos, la propagación de estados, la gestión de errores o la sincronización offline. Estas pruebas permitirán evaluar la consistencia funcional de la plataforma independientemente de la implementación concreta de los sistemas externos. Para asegurar la estabilidad y la repetibilidad de estos flujos en el tiempo, estas pruebas se integrarán en los pipelines de CI/CD, generando evidencias automáticas, métricas de cobertura y alertas tempranas ante regresiones funcionales.

Adicionalmente, se emplearán **validadores de JSON Schema** y **linters de OpenAPI/AsyncAPI**, que permiten detectar discrepancias estructurales o semánticas entre lo definido en el *Acuerdo de Interoperabilidad* y lo implementado en los servicios.

Pruebas de interoperabilidad

En las pruebas de interoperabilidad, cuyo objetivo es validar no solo la conectividad técnica sino también la coherencia semántica, la secuencia de intercambio entre sistemas y el comportamiento resiliente de THOT, se utilizará un conjunto de herramientas que permita reproducir fielmente las condiciones reales del ecosistema multiproveedor.

En primer lugar, **Postman** continuará utilizándose como herramienta de ejecución y automatización de llamadas conforme al protocolo de interoperabilidad (sandbox de lote 2). Este entorno de sandbox se complementará con **Pact**, que garantizará la validación bidireccional de los contratos, asegurando que las distintas implementaciones interpretan correctamente los estados, transiciones, reglas de idempotencia, formatos de evidencia, firmas digitales y los catálogos de errores.

Para asegurar la correcta interpretación del modelo de datos y de los estados del protocolo, se utilizarán **validadores de esquemas** JSON y **linters de OpenAPI** que faciliten la detección temprana de divergencias entre lo diseñado y lo implementado.

Asimismo, se empleará **Toxiproxy** para simular condiciones de red degradada —latencias elevadas, pérdida de paquetes o reconexiones— fundamentales para validar escenarios operativos propios del Lote 2 y del entorno real de campo, especialmente en sincronización offline, subida de ficheros o recuperación de transacciones.

Finalmente, la instrumentación mediante **Prometheus y Grafana**, junto con la centralización de logs en **Loki**, permitirá monitorizar con precisión el comportamiento del sistema durante las pruebas de interoperabilidad. Este conjunto de herramientas garantizará la trazabilidad extremo a extremo, la correlación completa de transacciones y la detección de discrepancias funcionales, así como el análisis detallado de latencias, errores, firmas, autenticaciones y secuencias de estado.