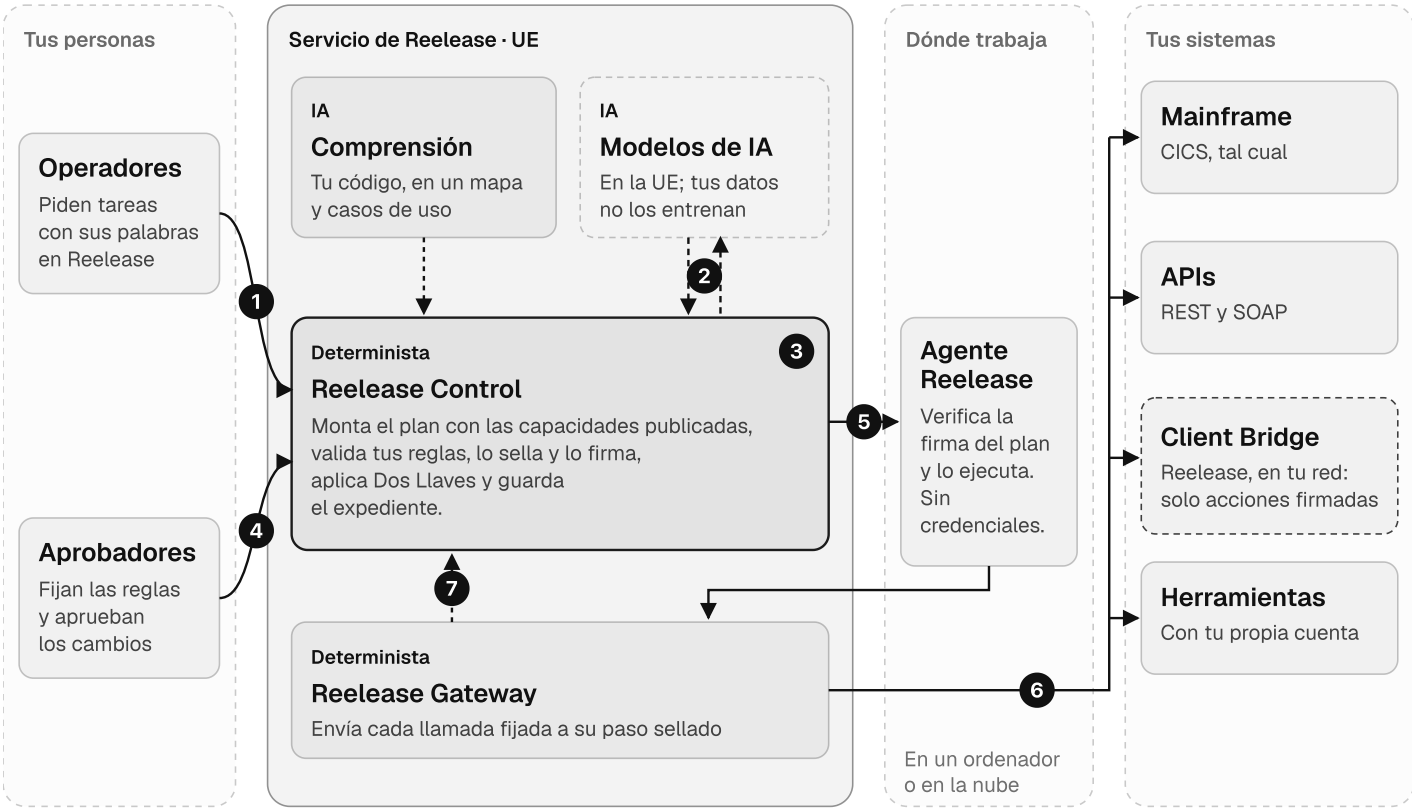
Ficha de seguridad de Reelease

Reelease es la capa de control entre la IA y tus sistemas: agentes que empiezan sin permisos, las aprobaciones que tú defines y un expediente de cada ejecución. Esta ficha reúne la arquitectura y los hechos que pide una revisión de proveedor.

Fecha de la ficha: 17 de noviembre de 2026



1. **Pedir.** Un operador pide la tarea con sus palabras.
2. **Proponer.** El modelo sugiere un plan.
3. **Sellar.** Tus reglas validan cada paso y el plan se firma.
4. **Aprobar.** Los cambios esperan a Dos Llaves.
5. **Ejecutar.** El agente verifica la firma y ejecuta.
6. **Llamar.** Tu sistema recibe la llamada sellada.
7. **Registrar.** Cada paso queda en el expediente.

Comprobar, sellar, aprobar y registrar lo hace Reelease, sin el modelo.

El servicio de Reelease funciona en Google Cloud, en Madrid, con la base de datos cifrada en Fráncfort. Las credenciales de conexión se guardan cifradas en Reelease y solo se usan para la llamada sellada.

PREGUNTA	RESPUESTA CORTA

PREGUNTA	RESPUESTA CORTA
Control de cada ejecución	
¿Con qué permisos empieza un agente?	Un agente nuevo empieza sin permisos: mínimo privilegio por defecto. Un administrador le activa cada capacidad.
¿Quién aprueba los pasos sensibles?	Tú decides qué pasos esperan a una persona y quién aprueba: supervisión humana (human-in-the-loop) en los pasos que tú eliges.
¿Puede el agente saltarse las reglas?	Las reglas son lo que el mercado llama guardrails: límites que el agente no puede saltarse. Lo que el sistema prohíbe, ningún agente lo puede permitir.
¿Cómo se para un agente?	Cualquier miembro con acceso completo a la plataforma y al agente lo suspende al momento. Solo un administrador lo reanuda.
Expediente de cada ejecución	
¿Qué queda de cada ejecución?	Cada ejecución deja su expediente, la pista de auditoría completa de la tarea: quién la lanzó, cada paso, cada aprobación y cada acción.
¿Se puede exportar y conservar?	Se exporta y se conserva aunque se borre el agente, con plazos de conservación por sistema y bloqueo legal.
¿Se registran los cambios de permisos?	Cada cambio de permisos queda registrado con quién, cuándo y por qué.
Identidad y credenciales	
¿Cómo acceden las personas?	Cuenta corporativa para cada persona. Segundo factor en todos los planes, obligatorio para todo tu equipo si lo decides.
¿Puedo usar mi proveedor de identidad?	En Piloto, Pro y Enterprise, acceso con tu proveedor de identidad (SSO): Microsoft Entra ID, Google Workspace, Okta u otro proveedor OpenID Connect.
¿Qué pasa al dar de baja a alguien?	Al dar de baja a alguien se revocan sus accesos, cuentas y ordenadores.
¿Dónde están las credenciales?	Las credenciales se guardan cifradas (AES-256) y nunca llegan al ordenador del operador.
Datos	
¿Se copian mis datos?	Tus datos se consultan, no se copian: el agente consulta en el momento lo que necesita.
¿Qué se guarda y cómo?	Se guardan cifrados la configuración, el conocimiento de tus sistemas y el expediente de cada ejecución.
¿Qué pasa con el código que aporto?	El código que aportas para el análisis se lee en un espacio temporal, y un ZIP se guarda como mucho 8 días.
¿Dónde están mis datos?	Residencia de datos en la UE: con nuestro servicio, la información de tus sistemas está en la Unión Europea, con los servicios en Madrid y la base de datos en Fráncfort.
Modelos de IA	
¿Quién elige el modelo?	Eliges el modelo para cada sistema y cada agente: los que ofrece Reelease, tu propio proveedor o un modelo abierto en tus servidores.
¿Se entrena con mis datos?	Ningún proveedor de IA entrena sus modelos con lo que lee el agente.
¿Y si el modelo no está disponible?	Si el modelo elegido no está disponible, la tarea se detiene: nunca pasa a otro proveedor.
¿Dónde trabajan los modelos de Reelease?	Los modelos que ofrece Reelease trabajan dentro de la Unión Europea.

PREGUNTA	RESPUESTA CORTA
Dónde funciona Reelease y dónde trabaja el agente	
¿Dónde funciona Reelease?	Reelease funciona como servicio en Madrid, en tu nube, en tus instalaciones o en modo aislado, sin ninguna conexión de salida.
¿Cómo se aísla cada ejecución en la nube?	En la nube, cada ejecución trabaja en su propio espacio desechable, sin acceso a internet ni a otras ejecuciones.
¿Y en el ordenador del operador?	En el ordenador del operador, el Agente Reelease trabaja en una carpeta aislada para cada ejecución. El escritorio se usa siempre con el consentimiento del operador.
Cumplimiento	
¿Con qué normas te ayuda?	Reelease está diseñado para ayudarte a cumplir el RGPD, el Reglamento europeo de IA, DORA y NIS2. **Reglamento europeo de IA** Arts. 12, 14 y 26 **DORA** Arts. 9 y 28 a 30 **RGPD** Arts. 5, 28 y 32 **NIS2** Art. 21
¿Quién hace la evaluación?	La evaluación de cumplimiento es tuya. Te damos los controles del producto, la trazabilidad de cada ejecución y la documentación para hacerla.
¿Y en el sector público?	Sector público: el Esquema Nacional de Seguridad lo aplica cada organismo, y Reelease se despliega en tus instalaciones si lo necesitas.
Aviso de fallos y plazos de respuesta	
¿Cómo se avisa de un fallo de seguridad?	Si encuentras un problema de seguridad, escríbenos a security@reelease.io con los pasos para reproducirlo. Confirmamos la recepción y te informamos hasta que queda resuelto.
¿En cuánto tiempo responde soporte?	Primera respuesta de soporte: en el Piloto, lo urgente en 4 horas laborables y el resto en 1 día laborable; en Pro, en menos de 1 hora; en Enterprise, por contrato.
¿En qué horario?	El horario es de lunes a viernes, de 9:00 a 18:00 (hora de Madrid), salvo festivos nacionales. Son objetivos de primera respuesta; el SLA contractual está disponible en Enterprise.

Textos legales

Encargo del tratamiento Subencargados Política de privacidad Información legal