

1. Datos en la Unión Europea

Toda la información se procesa y almacena dentro del Espacio Económico Europeo. No hay transferencias internacionales fuera de la UE, salvo el eventual acceso desde EE. UU. del servicio de monitorización de errores (Sentry), que no recibe datos personales, detallado en la relación de subencargados. Los proveedores de IA no usan los datos para entrenamiento; Amazon Bedrock y Google Vertex AI (con la caché de datos desactivada) no conservan las peticiones, y Mistral AI tampoco las conserva (retención cero de datos activada en la cuenta de Edilia Tech). Antes de enviar cualquier texto a los modelos de IA o a la búsqueda semántica, el servidor de Edilia Tech sustituye automáticamente por marcadores los DNI, NIE, NIF, IBAN, teléfonos, correos electrónicos, direcciones y nombres de persona que detecta, y vuelve a poner los datos reales en la respuesta. La detección no es infalible: puede no reconocer apellidos poco frecuentes escritos sueltos, datos narrados sin un formato reconocible o datos contenidos en imágenes. Las preguntas que contienen datos personales no se guardan en la caché de respuestas.

2. Medidas técnicas

- **Cifrado:** TLS 1.2 y 1.3 en tránsito; base de datos principal cifrada en reposo con AES-256 (incluidos los registros de transacciones y el registro binario); los campos narrativos de la diligencia debida de los partícipes se cifran además en la aplicación; copias de seguridad cifradas con GPG AES-256. Los ficheros subidos y la base de datos de búsqueda semántica no están cifrados en reposo.
- **Aislamiento por entidad:** control de acceso por roles; los datos de una entidad no son accesibles por otra.
- **Consultas parametrizadas** y sanitización de salida (sin inyección).
- **Cabeceras de seguridad** (HSTS con preload, política de seguridad de contenidos con frame-ancestors, X-Content-Type-Options, Referrer-Policy y Permissions-Policy) y límites de uso por usuario.
- **Monitorización** de errores y anomalías; copia de seguridad cifrada diaria de todo el servidor, guardada fuera de él (completa semanal e incremental diaria, con retención de cuatro semanas), y copia diaria cifrada de la base de datos.
- **Doble factor:** disponible para todos los usuarios en *Mi cuenta* y obligatorio en el panel de administración de Edilia Tech.
- **Seudonimización** automática de los datos personales antes de cualquier envío a los modelos de IA.
- **Registro de actividad** de las acciones de cada usuario, con la dirección IP seudonimizada, que el cliente puede consultar y que se borra a los 12 meses.

3. Confidencialidad de la información regulatoria

La información de cumplimiento que la entidad aporta se trata con confidencialidad reforzada, dado su carácter sensible en el ámbito de los mercados de valores. El acceso se limita a lo estrictamente necesario para prestar el servicio. Cuando el personal de Edilia Tech necesita entrar en la cuenta de un cliente (soporte o incidencias, o para registrar una decisión sobre una coincidencia del cribado a petición escrita del cliente), el administrador tiene que escribir el motivo, que queda en el registro de actividad que ve el propio cliente, y el permiso caduca a los 15 minutos.

4. Brechas de seguridad

En caso de incidente que afecte a datos personales, se notificará conforme a los arts. 33 y 34 del RGPD a la autoridad de control y, cuando proceda, a los afectados.

5. Contacto

Para cuestiones de seguridad o para comunicar una incidencia: contacto@edilia.tech.