

¿Qué normativas de la UE afectan a la selección de un proveedor de seguridad, más allá del GDPR?

Respuesta breve: Más allá del GDPR, tres regímenes de la UE están configurando cada vez más la selección de proveedores: DORA (resiliencia operativa para entidades financieras y sus proveedores de TIC), NIS2 (obligaciones de ciberseguridad para entidades esenciales e importantes, incluida la seguridad de la cadena de suministro) y la Ley de IA de la UE (normas escalonadas por riesgo para sistemas de IA). Cada una traslada obligaciones hacia los proveedores. El diseño de Cyber Crucible — sin recopilación de contenido del cliente, procesamiento local, opción on-premises — respalda las obligaciones del cliente en el marco de todas ellas, sin que Cyber Crucible reclame el cumplimiento en nombre del cliente.

El panorama de un vistazo

- **GDPR** — la base para el tratamiento de datos personales en toda la UE. Consulte la página del GDPR en las Guías de Cumplimiento por País.
- **DORA** — se aplica desde el 17 de enero de 2025 a las entidades financieras y, de manera importante, a sus proveedores externos de servicios de TIC.
- **NIS2** — los estados miembros debían transponerla antes de octubre de 2024; a partir de 2026 la mayoría lo ha hecho, mientras que varios seguían finalizando la legislación nacional.
- **Ley de IA de la UE** — obligaciones escalonadas por riesgo que se implementarán progresivamente hasta 2026-2027.

Cómo encaja Cyber Crucible

El tema recurrente es el riesgo de la cadena de suministro y de terceros. Dado que Cyber Crucible no recopila contenido, credenciales ni claves del cliente y puede ejecutarse completamente dentro del perímetro del cliente, reduce la superficie que estos regímenes están concebidos para controlar. Las páginas de este libro abordan cada régimen y los principales estados miembros. La documentación está disponible en dpo@cybercrucible.com.

