Guías de riesgo de proveedores de la Unión Europea y los Estados miembros

Cómo Cyber Crucible respalda los regímenes de toda la UE (GDPR, DORA, NIS2, la Ley de IA) y las particularidades de los estados miembros (Alemania, Francia, Irlanda, Países Bajos, España, Italia, Polonia, Suecia) desde una perspectiva de selección de proveedores. Indica claramente lo que Cyber Crucible posee y no posee, y no hace promesas de cumplimiento en nombre del cliente.

¿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**.

¿Cómo respalda Cyber Crucible a las entidades financieras de la UE en el marco de DORA?

Respuesta breve: Cyber Crucible es un proveedor externo de servicios TIC en los términos de DORA, y respalda las obligaciones de DORA de una entidad financiera —controles contractuales, información sobre incidentes y pruebas de resiliencia— a la vez que reduce el riesgo de terceros TIC, ya que nunca recopila los datos de la entidad. DORA se aplica desde el 17 de enero de 2025. Cyber Crucible no afirma ser "conforme a DORA" en nombre de un cliente; el cumplimiento corresponde a la entidad financiera, y Cyber Crucible proporciona el respaldo y las evidencias que su programa necesita.

Cómo respalda el programa DORA de la entidad

- **Reducción del riesgo TIC.** No se recopila ningún contenido, credenciales ni claves del cliente, y la protección se ejecuta localmente, reduciendo la superficie de ataque de terceros que DORA busca abordar.
- **Controles contractuales.** Cyber Crucible puede adaptarse a las disposiciones contractuales que DORA exige para los acuerdos con proveedores externos de servicios TIC (seguridad, cooperación en incidentes, derechos de auditoría e información, transparencia en la subcontratación).
- **Cooperación en incidentes.** Un proceso documentado de respuesta a brechas proporciona información oportuna y con valor probatorio, y se ofrece contractualmente un plazo de notificación comprometido para respaldar las obligaciones de la entidad en materia de reporte de incidentes.
- **Resiliencia.** La protección de endpoints continúa funcionando durante una interrupción del backend de gestión, lo cual respalda los objetivos de resiliencia operativa.

El límite honesto

DORA también permite que las Autoridades Europeas de Supervisión designen proveedores externos de servicios TIC **críticos** (CTPP, por sus siglas en inglés) para su supervisión directa a nivel de la UE. Cyber Crucible no está designado como CTPP y no se presenta como tal. Respalda las obligaciones de la entidad financiera; no las asume.

¿Cómo respalda Cyber Crucible las obligaciones de NIS2 para entidades esenciales e importantes?

Respuesta breve: Para una organización clasificada como entidad esencial o importante en virtud de NIS2, Cyber Crucible respalda las medidas de gestión de riesgos exigidas —protección de endpoints, control de acceso, cifrado y gestión de incidentes— y respalda las expectativas de seguridad de la cadena de suministro de la directiva, ya que no recopila datos de clientes y puede ejecutarse dentro del perímetro de la entidad. Cyber Crucible respalda estas obligaciones; no las certifica ni las asume.

Cómo respalda las medidas de NIS2

- **Medidas de gestión de riesgos de ciberseguridad.** La prevención autónoma de endpoints, el acceso respaldado por MFA y el cifrado corresponden a varias de las medidas básicas de la directiva.
- **Seguridad de la cadena de suministro.** Como proveedor que no recopila contenido de clientes y ofrece implementación en las instalaciones (on-premises), Cyber Crucible reduce, en lugar de añadir, el riesgo de la cadena de suministro que NIS2 exige gestionar a las entidades.
- **Soporte para la gestión y notificación de incidentes.** Un proceso documentado de respuesta ante brechas ayuda a la entidad a cumplir con los plazos de alerta temprana y notificación de NIS2.

El límite honesto

Las obligaciones de NIS2 recaen en la entidad esencial o importante, no en una herramienta de seguridad individual. La transposición por parte de los Estados miembros varió: para 2026, la mayoría de los estados habían transpuesto la directiva a su legislación nacional, mientras que varios —incluidos Francia, Irlanda, los Países Bajos y España— aún la estaban finalizando. Cyber Crucible no posee ninguna "certificación" NIS2; proporciona evidencia de controles de respaldo bajo acuerdo de confidencialidad (NDA).

¿Cómo se relaciona Cyber Crucible con la Ley de IA de la UE?

Respuesta breve: Cyber Crucible utiliza IA únicamente durante el desarrollo (su trabajo de descubrimiento con Genetic AI) y ejecuta heurísticas fijas y deterministas en tiempo de ejecución; no existe un modelo de IA en vivo que tome decisiones en el endpoint del cliente. Por lo tanto, Cyber Crucible no incorpora un sistema de IA de alto riesgo o de propósito general en el entorno del cliente. El cliente sigue siendo responsable de evaluar sus propias obligaciones conforme a la Ley de IA de la UE, cuyos requisitos se implementarán de forma progresiva hasta 2026-2027.

Por qué importa la arquitectura en este caso

- **No se despliega ningún sistema de IA en tiempo de ejecución en el cliente.** El endpoint ejecuta heurísticas deterministas a nivel de kernel, no un modelo en vivo, por lo que no existe un sistema de IA en el dispositivo que el cliente deba clasificar y gobernar conforme a la Ley.
- **Solo en tiempo de desarrollo.** El trabajo de IA se realiza en el entorno interno de desarrollo de Cyber Crucible, utilizando conjuntos de datos de investigación internos; no se utiliza contenido, credenciales ni claves del cliente para entrenar, alimentar o ajustar un modelo.
- **Transparencia.** Dado que el comportamiento en tiempo de ejecución es determinista y comprobable en lugar de probabilístico, resulta sencillo describirlo y documentarlo.

El límite honesto

Cyber Crucible no afirma que el producto sea "conforme con la Ley de IA de la UE" ni realiza esa determinación en nombre del cliente. Esta página describe cómo funciona el producto para que la propia evaluación del cliente respecto a la Ley de IA pueda tenerlo en cuenta con precisión. Esto no constituye asesoramiento legal.

¿Cómo respalda Cyber Crucible los requisitos de protección de datos y seguridad en Alemania?

Respuesta breve: En Alemania, Cyber Crucible respalda las obligaciones de una organización en virtud del GDPR y la Ley Federal de Protección de Datos (BDSG) al no recopilar contenido, credenciales ni claves de los clientes, y al procesar en el endpoint. Para las organizaciones que están dentro del alcance del régimen de ciberseguridad de Alemania (el marco de la Ley BSI, en su adopción de la NIS2), el diseño de procesamiento local con capacidad de implementación local (on-premises) respalda sus obligaciones de seguridad y de cadena de suministro.

Cómo se alinea

- **GDPR + BDSG.** La minimización de datos, el cifrado y el control de acceso respaldan la base de protección de datos alemana; hay disponible un acuerdo de procesamiento de datos.
- **Residencia de datos.** La implementación local (on-premises) mantiene los datos personales en Alemania cuando así se requiere; ningún contenido del cliente se transfiere al extranjero para el procesamiento de seguridad.
- **Régimen de ciberseguridad.** Alemania ha estado transponiendo la NIS2 a su marco de la Ley BSI; Cyber Crucible respalda las medidas de gestión de riesgos y de cadena de suministro de las entidades cubiertas.

El límite honesto

El cumplimiento recae en la organización y, cuando corresponda, en su responsable de protección de datos (DPO) y en la autoridad supervisora competente. Cyber Crucible no posee ninguna certificación alemana y respalda estas obligaciones, en lugar de asumirlas. La documentación está disponible a solicitud.

¿Cómo respalda Cyber Crucible los requisitos de protección de datos en Francia?

Respuesta breve: En Francia, Cyber Crucible respalda las obligaciones de una organización conforme al GDPR y a la Loi Informatique et Libertés (aplicada por la CNIL) minimizando los datos y el procesamiento a nivel local. Dado que no recopila contenido de clientes, credenciales ni claves, la mayoría de las obligaciones que aplica la CNIL tienen una superficie mínima en su custodia.

Cómo se alinea

- **GDPR + legislación nacional.** El cifrado, el control de acceso y la minimización de datos respaldan la base normativa francesa; hay disponible un acuerdo de procesamiento de datos.
- **Residencia de datos.** El despliegue on-premises mantiene los datos personales en Francia cuando así se requiere.
- **Régimen de ciberseguridad.** La transposición de NIS2 en Francia aún estaba en trámite legislativo a fecha de 2026; Cyber Crucible respalda las medidas de seguridad y de cadena de suministro de las entidades cubiertas según el marco tal como sea adoptado.

El límite honesto

La CNIL es una autoridad supervisora activa; el cumplimiento es responsabilidad de la organización, y Cyber Crucible lo respalda sin reivindicar una certificación francesa. La documentación está disponible bajo solicitud.

¿Cómo respalda Cyber Crucible los requisitos de protección de datos en Irlanda?

Respuesta breve: En Irlanda, Cyber Crucible respalda las obligaciones de una organización en virtud del RGPD y la Ley de Protección de Datos de 2018 (Data Protection Act 2018) (aplicada por la Data Protection Commission) al no recopilar contenido de clientes, credenciales ni claves, y al procesar los datos en el endpoint. Irlanda es la autoridad supervisora principal para muchas multinacionales, lo que eleva el nivel de escrutinio hacia los proveedores; la huella de datos mínima mantiene el riesgo del proveedor bajo.

Cómo se alinea

- **RGPD + DPA 2018.** La minimización de datos, el cifrado y el control de acceso respaldan la base irlandesa; hay disponible un acuerdo de tratamiento de datos.
- **Residencia de datos.** La implementación local (on-premises) mantiene los datos personales en Irlanda cuando así se requiere.
- **Régimen de ciberseguridad.** La transposición de NIS2 en Irlanda aún se estaba finalizando a partir de 2026; Cyber Crucible respalda las medidas de las entidades cubiertas conforme al marco tal como se adopte.

El límite honesto

La Data Protection Commission es una autoridad principal destacada en la UE; el cumplimiento es responsabilidad de la organización. Cyber Crucible no posee ninguna certificación irlandesa y respalda estas obligaciones. La documentación está disponible a solicitud.

¿Cómo respalda Cyber Crucible los requisitos de protección de datos en los Países Bajos?

Respuesta breve: En los Países Bajos, Cyber Crucible respalda las obligaciones de una organización en virtud del RGPD y la Ley de Implementación del RGPD neerlandesa (aplicada por la Autoriteit Persoonsgegevens) al minimizar los datos y el procesamiento en el endpoint. No recopila contenido del cliente, credenciales ni claves, por lo que la mayoría de las obligaciones tienen poca superficie bajo su custodia.

Cómo se alinea

- **RGPD + implementación nacional.** El cifrado, el control de acceso y la minimización de datos respaldan la línea base neerlandesa; hay disponible un acuerdo de tratamiento de datos.
- **Residencia de datos.** La implementación local (on-premises) mantiene los datos personales en los Países Bajos cuando así se requiere.
- **Régimen de ciberseguridad.** La transposición neerlandesa de NIS2 (la Cyberbeveiligingswet) aún estaba en proceso de finalización a partir de 2026; Cyber Crucible respalda las medidas de las entidades cubiertas conforme al marco tal como se adopte.

El límite honesto

El cumplimiento recae en la organización y en la Autoriteit Persoonsgegevens cuando corresponda. Cyber Crucible no posee ninguna certificación neerlandesa y respalda estas obligaciones. La documentación está disponible bajo solicitud.

¿Cómo respalda Cyber Crucible los requisitos de protección de datos en España?

Respuesta breve: En España, Cyber Crucible respalda las obligaciones de una organización en virtud del RGPD y la Ley Orgánica de Protección de Datos (LOPDGDD, cuyo cumplimiento aplica la AEPD) al no recopilar contenido del cliente, credenciales ni claves, y al procesar la información de forma local. Dado que hay una cantidad mínima de datos personales bajo su custodia, la mayoría de las obligaciones que aplica la AEPD tienen poco a lo que atenerse.

Cómo se alinea

- **RGPD + LOPDGDD.** La minimización de datos, el cifrado y el control de acceso respaldan la base española; hay disponible un acuerdo de tratamiento de datos.
- **Residencia de datos.** La implementación local (on-premises) mantiene los datos personales en España cuando así se requiere.
- **Régimen de ciberseguridad.** La transposición de NIS2 en España aún estaba en proceso legislativo a partir de 2026; Cyber Crucible respalda las medidas de las entidades cubiertas conforme al marco tal como se adopte.

El límite honesto

La AEPD es uno de los organismos de cumplimiento más activos de la UE; el cumplimiento es responsabilidad de la organización. Cyber Crucible no posee ninguna certificación española y respalda estas obligaciones. La documentación está disponible a solicitud.

¿Cómo respalda Cyber Crucible los requisitos de protección de datos en Italia?

Respuesta breve: En Italia, Cyber Crucible respalda las obligaciones de una organización en virtud del GDPR y del Código de Privacidad italiano (aplicado por el Garante) al minimizar los datos y el procesamiento en el endpoint. No recopila contenido, credenciales ni claves del cliente, por lo que la mayoría de las obligaciones tienen una superficie mínima bajo su custodia.

Cómo se alinea

- **GDPR + Código de Privacidad.** El cifrado, el control de acceso y la minimización de datos respaldan la base italiana; hay disponible un acuerdo de tratamiento de datos.
- **Residencia de datos.** La implementación local mantiene los datos personales en Italia cuando así se requiere.
- **Régimen de ciberseguridad.** Italia estuvo entre los primeros estados miembros en transponer NIS2 a la legislación nacional; Cyber Crucible respalda las medidas de gestión de riesgos y de la cadena de suministro de las entidades cubiertas.

El límite honesto

El Garante es una autoridad de supervisión activa; el cumplimiento es responsabilidad de la organización. Cyber Crucible no posee ninguna certificación italiana y respalda estas obligaciones. La documentación está disponible a solicitud.

¿Cómo respalda Cyber Crucible los requisitos de protección de datos en Polonia?

Respuesta breve: En Polonia, Cyber Crucible respalda las obligaciones de una organización en virtud del GDPR y la Ley de Protección de Datos Personales de Polonia (aplicada por la UODO) al no recopilar contenido del cliente, credenciales ni claves, y al procesar los datos en el endpoint. La huella mínima de datos mantiene la mayoría de las obligaciones con una superficie reducida.

Cómo se alinea

- **GDPR + legislación nacional.** La minimización de datos, el cifrado y el control de acceso respaldan la base polaca; hay disponible un acuerdo de procesamiento de datos.
- **Residencia de datos.** La implementación en las instalaciones mantiene los datos personales en Polonia cuando así se requiere.
- **Régimen de ciberseguridad.** Polonia ha estado actualizando su marco del Sistema Nacional de Ciberseguridad (KSC) para reflejar la NIS2; Cyber Crucible respalda las medidas de las entidades cubiertas bajo el marco tal como se adopte.

El límite honesto

El cumplimiento recae en la organización y en la UODO cuando corresponda. Cyber Crucible no posee ninguna certificación polaca y respalda estas obligaciones. La documentación está disponible previa solicitud.

¿Cómo respalda Cyber Crucible los requisitos de protección de datos en Suecia y los países nórdicos?

Respuesta breve: En Suecia y en la región nórdica en general, Cyber Crucible respalda las obligaciones de una organización conforme al GDPR y las leyes nacionales de implementación (en Suecia, aplicadas por la IMY) al minimizar los datos y el procesamiento en el endpoint. Dado que no recopila contenido de clientes, credenciales ni claves, la mayoría de las obligaciones tienen poca incidencia en su custodia.

Cómo se alinea

- **GDPR + implementación nacional.** El cifrado, el control de acceso y la minimización de datos respaldan la línea base nórdica; hay disponible un acuerdo de tratamiento de datos.
- **Residencia de datos.** La implementación local (on-premises) mantiene los datos personales dentro del país cuando así se requiere.
- **Régimen de ciberseguridad.** Los estados miembros nórdicos han estado transponiendo NIS2 a su legislación nacional según sus propios plazos; Cyber Crucible respalda las medidas de las entidades cubiertas conforme al marco tal como se adopte.

El límite honesto

El cumplimiento recae en la organización y en la autoridad de supervisión nacional pertinente. Cyber Crucible no posee ninguna certificación nacional en ningún país nórdico y respalda estas obligaciones, en lugar de asumirlas. La documentación está disponible a solicitud.