

Guias de Risco de Fornecedores da União Europeia e dos Estados-Membros

Como a Cyber Crucible apoia os regimes de âmbito europeu (GDPR, DORA, NIS2, o AI Act) e as especificidades de cada Estado-Membro (Alemanha, França, Irlanda, Países Baixos, Espanha, Itália, Polónia, Suécia) numa perspetiva de seleção de fornecedores. Declara claramente o que a Cyber Crucible detém e não detém, e não faz quaisquer promessas de conformidade em nome do cliente.

- [Quais regras da UE afetam a seleção de um fornecedor de segurança, além do GDPR?](#)
- [Como a Cyber Crucible apoia as entidades financeiras da UE no âmbito da DORA?](#)
- [Como é que a Cyber Crucible apoia as obrigações da NIS2 para entidades essenciais e importantes?](#)
- [Como o Cyber Crucible se relaciona com a Lei de IA da UE?](#)
- [Como é que a Cyber Crucible apoia os requisitos de proteção de dados e segurança na Alemanha?](#)
- [Como a Cyber Crucible apoia os requisitos de proteção de dados na França?](#)
- [Como o Cyber Crucible oferece suporte aos requisitos de proteção de dados na Irlanda?](#)
- [Como a Cyber Crucible apoia os requisitos de proteção de dados nos Países Baixos?](#)
- [Como é que a Cyber Crucible apoia os requisitos de proteção de dados em Espanha?](#)
- [Como a Cyber Crucible apoia os requisitos de proteção de dados na Itália?](#)
- [Como a Cyber Crucible apoia os requisitos de proteção de dados na Polónia?](#)
- [Como a Cyber Crucible apoia os requisitos de proteção de dados na Suécia e nos países nórdicos?](#)

Quais regras da UE afetam a seleção de um fornecedor de segurança, além do GDPR?

Resposta curta: Além do GDPR, três regimes da UE moldam cada vez mais a seleção de fornecedores: o DORA (resiliência operacional para entidades financeiras e seus prestadores de TIC), o NIS2 (obrigações de cibersegurança para entidades essenciais e importantes, incluindo a segurança da cadeia de suprimentos) e o EU AI Act (regras escalonadas por risco para sistemas de IA). Cada um deles impõe obrigações aos fornecedores. O design da Cyber Crucible — sem coleta de conteúdo do cliente, processamento local, opção on-premises — apoia as obrigações do cliente em relação a todos eles, sem que a Cyber Crucible reivindique conformidade em nome do cliente.

Panorama geral

- **GDPR** — a base para o processamento de dados pessoais em toda a UE. Consulte os Guias de Conformidade por País para a página do GDPR.
- **DORA** — aplica-se a partir de 17 de janeiro de 2025 a entidades financeiras e, de forma importante, aos seus prestadores terceirizados de serviços de TIC.
- **NIS2** — os Estados-Membros deveriam transpô-lo até outubro de 2024; a partir de 2026, a maioria já o fez, embora vários ainda estivessem finalizando a legislação nacional.
- **EU AI Act** — obrigações escalonadas por risco, em fase de implementação até 2026–2027.

Como a Cyber Crucible se encaixa

O tema recorrente é o risco de cadeia de suprimentos e de terceiros. Como a Cyber Crucible não coleta conteúdo do cliente, credenciais ou chaves, e pode operar inteiramente dentro do perímetro do cliente, ela reduz a superfície que esses regimes foram elaborados para controlar. As páginas deste livro abordam cada regime e os principais Estados-Membros. A documentação está disponível em **dpo@cybercrucible.com**.

Como a Cyber Crucible apoia as entidades financeiras da UE no âmbito da DORA?

Resposta breve: A Cyber Crucible é um prestador terceiro de serviços TIC nos termos da DORA, e apoia as obrigações da DORA de uma entidade financeira — controlos contratuais, informação sobre incidentes e testes de resiliência — ao mesmo tempo que reduz o risco de terceiros TIC, pois nunca recolhe os dados da entidade. A DORA aplica-se a partir de 17 de janeiro de 2025. A Cyber Crucible não afirma estar "em conformidade com a DORA" em nome de um cliente; a conformidade é responsabilidade da entidade financeira, e a Cyber Crucible fornece o apoio e as evidências de que o seu programa necessita.

Como apoia o programa DORA da entidade

- **Redução do risco TIC.** Não é recolhido qualquer conteúdo, credenciais ou chaves do cliente, e a proteção funciona localmente — reduzindo a superfície de ataque de terceiros que a DORA visa.
- **Controlos contratuais.** A Cyber Crucible pode acomodar as disposições contratuais que a DORA exige para os acordos com prestadores terceiros de serviços TIC (segurança, cooperação em caso de incidentes, direitos de auditoria e informação, transparência de subcontratação).
- **Cooperação em incidentes.** Um processo documentado de resposta a violações fornece informação rápida e com valor probatório, e um prazo de notificação comprometido está disponível por contrato para apoiar os deveres de comunicação de incidentes da entidade.
- **Resiliência.** A proteção de endpoint continua a funcionar durante uma indisponibilidade do backend de gestão, o que apoia os objetivos de resiliência operacional.

O limite honesto

A DORA também permite que as Autoridades Europeias de Supervisão designem prestadores terceiros de serviços TIC **críticos** (CTPPs) para supervisão direta pela UE. A Cyber Crucible não está designada como CTPP e não se apresenta como tal. Apoia as obrigações da entidade financeira; não as assume.

Como é que a Cyber Crucible apoia as obrigações da NIS2 para entidades essenciais e importantes?

Resposta curta: Para uma organização classificada como entidade essencial ou importante ao abrigo da NIS2, a Cyber Crucible apoia as medidas de gestão de risco exigidas — proteção de endpoints, controlo de acesso, encriptação e gestão de incidentes — e apoia as expectativas da diretiva em matéria de segurança da cadeia de fornecimento, uma vez que não recolhe dados de clientes e pode ser executada dentro do perímetro da entidade. A Cyber Crucible apoia estas obrigações; não as certifica nem as assume.

Como apoia as medidas da NIS2

- **Medidas de gestão de risco de cibersegurança.** A prevenção autónoma em endpoints, o acesso reforçado por MFA e a encriptação correspondem a várias das medidas de base da diretiva.
- **Segurança da cadeia de fornecimento.** Como fornecedor que não recolhe conteúdo de clientes e que oferece implementação no local (on-premises), a Cyber Crucible reduz, em vez de acrescentar, o risco de cadeia de fornecimento que a NIS2 exige que as entidades geridam.
- **Apoio à gestão e notificação de incidentes.** Um processo documentado de resposta a violações ajuda a entidade a cumprir os prazos de alerta precoce e de notificação da NIS2.

O limite honesto

As obrigações da NIS2 recaem sobre a entidade essencial ou importante, e não sobre uma ferramenta de segurança individual. A transposição pelos Estados-Membros variou: em 2026, a maioria dos Estados já tinha transposto a diretiva para o direito nacional, enquanto vários — incluindo a França, a Irlanda, os Países Baixos e a Espanha — ainda a estavam a finalizar. A Cyber Crucible não detém qualquer "certificação" NIS2; fornece evidências de controlo de apoio sob NDA.

Como o Cyber Crucible se relaciona com a Lei de IA da UE?

Resposta breve: O Cyber Crucible utiliza IA apenas durante o desenvolvimento (o seu trabalho de descoberta com Genetic AI) e executa heurísticas fixas e determinísticas em tempo de execução — não existe um modelo de IA ativo a tomar decisões no endpoint do cliente. Assim, o Cyber Crucible não introduz um sistema de IA de alto risco ou de finalidade geral no ambiente do cliente. O cliente continua responsável por avaliar as suas próprias obrigações ao abrigo da Lei de IA da UE, cujos requisitos entrarão progressivamente em vigor até 2026–2027.

Por que motivo a arquitetura é relevante aqui

- **Nenhum sistema de IA em tempo de execução é implementado no cliente.** O endpoint executa heurísticas determinísticas do kernel, e não um modelo ativo — pelo que não existe nenhum sistema de IA no dispositivo que o cliente tenha de classificar e governar ao abrigo da Lei.
- **Apenas em tempo de desenvolvimento.** O trabalho de IA ocorre no ambiente interno de desenvolvimento do Cyber Crucible, com base em conjuntos de dados de investigação internos; nenhum conteúdo, credencial ou chave do cliente é utilizado para treinar, alimentar ou ajustar um modelo.
- **Transparência.** Uma vez que o comportamento em tempo de execução é determinístico e testável, em vez de probabilístico, é simples descrevê-lo e documentá-lo.

O limite honesto

O Cyber Crucible não afirma que o produto está "em conformidade com a Lei de IA da UE", nem faz essa determinação em nome do cliente. Esta página descreve o funcionamento do produto para que a própria avaliação do cliente relativa à Lei de IA a possa refletir com precisão. Isto não constitui aconselhamento jurídico.

Como é que a Cyber Crucible apoia os requisitos de proteção de dados e segurança na Alemanha?

Resposta breve: Na Alemanha, a Cyber Crucible apoia as obrigações de uma organização ao abrigo do RGPD e da Lei Federal de Proteção de Dados (BDSG - Bundesdatenschutzgesetz) ao não recolher conteúdo do cliente, credenciais ou chaves, processando os dados no endpoint. Para organizações abrangidas pelo regime de cibersegurança da Alemanha (o enquadramento da Lei BSI, à medida que incorpora a NIS2), o design de processamento local, com capacidade para implementação on-premises, apoia as suas obrigações de segurança e de cadeia de fornecimento.

Como se alinha

- **RGPD + BDSG.** A minimização de dados, a encriptação e o controlo de acesso apoiam a base de referência alemã de proteção de dados; está disponível um acordo de processamento de dados.
- **Residência dos dados.** A implementação on-premises mantém os dados pessoais na Alemanha quando exigido; nenhum conteúdo do cliente é transferido para fora do país para processamento de segurança.
- **Regime de cibersegurança.** A Alemanha tem vindo a transpor a NIS2 para o seu enquadramento da Lei BSI; a Cyber Crucible apoia as medidas de gestão de risco e de cadeia de fornecimento das entidades abrangidas.

O limite honesto

A conformidade é da responsabilidade da organização e, quando relevante, do seu encarregado de proteção de dados e da autoridade de supervisão competente. A Cyber Crucible não possui qualquer certificação alemã e apoia, em vez de assumir, estas obrigações. A documentação está disponível mediante pedido.

Como a Cyber Crucible apoia os requisitos de proteção de dados na França?

Resposta curta: Na França, a Cyber Crucible apoia as obrigações de uma organização no âmbito do GDPR e da Loi Informatique et Libertés (aplicada pela CNIL) ao minimizar dados e processamento localmente. Como não coleta conteúdo de clientes, credenciais ou chaves, a maioria das obrigações que a CNIL aplica tem superfície mínima sob sua custódia.

Como se alinha

- **GDPR + legislação nacional.** Criptografia, controle de acesso e minimização de dados apoiam a base francesa; um acordo de processamento de dados está disponível.
- **Residência de dados.** A implantação on-premises mantém os dados pessoais na França onde exigido.
- **Regime de cibersegurança.** A transposição do NIS2 pela França ainda estava em tramitação legislativa em 2026; a Cyber Crucible apoia as medidas de segurança e de cadeia de suprimentos das entidades abrangidas conforme a estrutura for adotada.

O limite honesto

A CNIL é uma autoridade supervisora ativa; a conformidade é responsabilidade da organização, e a Cyber Crucible a apoia sem alegar uma certificação francesa. A documentação está disponível mediante solicitação.

Como o Cyber Crucible oferece suporte aos requisitos de proteção de dados na Irlanda?

Resposta curta: Na Irlanda, o Cyber Crucible apoia as obrigações de uma organização no âmbito do GDPR e do Data Protection Act 2018 (aplicado pela Data Protection Commission), não coletando conteúdo, credenciais ou chaves do cliente e realizando o processamento no endpoint. A Irlanda é a autoridade supervisora principal para muitas multinacionais, o que eleva o padrão de escrutínio de fornecedores; a pegada mínima de dados mantém o lado do fornecedor com baixo risco.

Como está alinhado

- **GDPR + DPA 2018.** A minimização de dados, a criptografia e o controle de acesso apoiam o padrão irlandês; um acordo de processamento de dados está disponível.
- **Residência de dados.** A implantação on-premises mantém os dados pessoais na Irlanda quando exigido.
- **Regime de cibersegurança.** A transposição do NIS2 pela Irlanda ainda estava sendo finalizada em 2026; o Cyber Crucible apoia as medidas das entidades abrangidas conforme a estrutura adotada.

O limite honesto

A Data Protection Commission é uma autoridade líder proeminente na UE; a conformidade é responsabilidade da organização. O Cyber Crucible não possui certificação irlandesa e apoia esses deveres. A documentação está disponível mediante solicitação.

Como a Cyber Crucible apoia os requisitos de proteção de dados nos Países Baixos?

Resposta curta: Nos Países Baixos, a Cyber Crucible apoia as obrigações de uma organização no âmbito do GDPR e da Lei de Implementação do GDPR neerlandesa (aplicada pela Autoriteit Persoonsgegevens), minimizando os dados e o processamento no endpoint. Não recolhe conteúdo de clientes, credenciais ou chaves, pelo que a maioria das obrigações tem pouca superfície na sua custódia.

Como se alinha

- **GDPR + implementação nacional.** A encriptação, o controlo de acesso e a minimização de dados apoiam a base neerlandesa; está disponível um acordo de processamento de dados.
- **Residência de dados.** A implementação no local mantém os dados pessoais nos Países Baixos, quando exigido.
- **Regime de cibersegurança.** A transposição do NIS2 nos Países Baixos (a Cyberbeveiligingswet) ainda estava a ser finalizada em 2026; a Cyber Crucible apoia as medidas das entidades abrangidas ao abrigo do enquadramento tal como adotado.

O limite honesto

A conformidade é da responsabilidade da organização e, quando aplicável, da Autoriteit Persoonsgegevens. A Cyber Crucible não possui qualquer certificação neerlandesa e apoia estas obrigações. A documentação está disponível mediante pedido.

Como é que a Cyber Crucible apoia os requisitos de proteção de dados em Espanha?

Resposta breve: Em Espanha, a Cyber Crucible apoia as obrigações de uma organização ao abrigo do RGPD e da Lei Orgânica de Proteção de Dados (LOPDGDD, aplicada pela AEPD), não recolhendo conteúdo de clientes, credenciais ou chaves, e processando localmente. Uma vez que existem dados pessoais mínimos sob a sua custódia, a maioria das obrigações que a AEPD faz cumprir tem pouco a que se aplicar.

Como se alinha

- **RGPD + LOPDGDD.** A minimização de dados, a encriptação e o controlo de acesso apoiam a base espanhola; está disponível um acordo de processamento de dados.
- **Residência de dados.** A implementação on-premises mantém os dados pessoais em Espanha sempre que exigido.
- **Regime de cibersegurança.** A transposição da NIS2 em Espanha ainda estava em processo legislativo em 2026; a Cyber Crucible apoia as medidas das entidades abrangidas ao abrigo do enquadramento tal como adotado.

O limite honesto

A AEPD é uma das autoridades de aplicação mais ativas da UE; a conformidade é da responsabilidade da organização. A Cyber Crucible não detém qualquer certificação espanhola e apoia estas obrigações. A documentação está disponível mediante pedido.

Como a Cyber Crucible apoia os requisitos de proteção de dados na Itália?

Resposta curta: Na Itália, a Cyber Crucible apoia as obrigações de uma organização ao abrigo do GDPR e do Código de Privacidade italiano (aplicado pelo Garante) ao minimizar os dados e o processamento no endpoint. Não recolhe conteúdo do cliente, credenciais ou chaves, pelo que a maioria das obrigações tem uma superfície mínima sob a sua custódia.

Como se alinha

- **GDPR + Código de Privacidade.** A encriptação, o controlo de acesso e a minimização de dados apoiam a base italiana; está disponível um acordo de processamento de dados.
- **Residência de dados.** A implementação no local mantém os dados pessoais na Itália quando exigido.
- **Regime de cibersegurança.** A Itália foi um dos primeiros Estados-Membros a transpor a NIS2 para a legislação nacional; a Cyber Crucible apoia as medidas de gestão de risco e de cadeia de fornecimento das entidades abrangidas.

O limite honesto

O Garante é uma autoridade de supervisão ativa; a conformidade é da responsabilidade da organização. A Cyber Crucible não possui nenhuma certificação italiana e apoia estas obrigações. A documentação está disponível mediante pedido.

Como a Cyber Crucible apoia os requisitos de proteção de dados na Polônia?

Resposta breve: Na Polônia, a Cyber Crucible apoia as obrigações de uma organização no âmbito do GDPR e da Lei de Proteção de Dados Pessoais polaca (aplicada pela UODO) ao não recolher conteúdo, credenciais ou chaves de clientes, e ao processar os dados no endpoint. A pegada de dados mínima mantém a maioria das obrigações com baixa superfície de exposição.

Como se alinha

- **GDPR + legislação nacional.** A minimização de dados, a encriptação e o controlo de acesso apoiam a base de referência polaca; está disponível um acordo de processamento de dados.
- **Residência de dados.** A implementação on-premises mantém os dados pessoais na Polónia sempre que exigido.
- **Regime de cibersegurança.** A Polónia tem vindo a atualizar o seu quadro do Sistema Nacional de Cibersegurança (KSC) para refletir a NIS2; a Cyber Crucible apoia as medidas das entidades abrangidas no âmbito do quadro conforme adotado.

O limite honesto

A conformidade é da responsabilidade da organização e, quando relevante, da UODO. A Cyber Crucible não detém nenhuma certificação polaca e apoia estes deveres. A documentação está disponível mediante solicitação.

Como a Cyber Crucible apoia os requisitos de proteção de dados na Suécia e nos países nórdicos?

Resposta breve: Na Suécia e na região nórdica em geral, a Cyber Crucible apoia as obrigações de uma organização ao abrigo do GDPR e das leis nacionais de aplicação (na Suécia, fiscalizadas pela IMY) através da minimização dos dados e do processamento no endpoint. Uma vez que não recolhe conteúdo de clientes, credenciais ou chaves, a maioria das obrigações tem pouca relevância no que respeita à sua custódia.

Como se alinha

- **GDPR + implementação nacional.** A encriptação, o controlo de acesso e a minimização de dados apoiam a base nórdica; está disponível um acordo de processamento de dados.
- **Residência de dados.** A implementação no local (on-premises) mantém os dados pessoais dentro do país, quando exigido.
- **Regime de cibersegurança.** Os Estados-membros nórdicos têm vindo a transpor a NIS2 para a legislação nacional segundo os seus próprios calendários; a Cyber Crucible apoia as medidas das entidades abrangidas ao abrigo do enquadramento adotado.

O limite honesto

A conformidade é da responsabilidade da organização e da autoridade nacional de supervisão relevante. A Cyber Crucible não detém qualquer certificação nacional em nenhum país nórdico e apoia, em vez de assumir, estas obrigações. A documentação está disponível mediante pedido.