

Guias Internacionais de Risco de Fornecedores

Respostas sobre risco de fornecedores por país, além dos guias existentes para o Golfo, África e UE/Reino Unido — Canadá, Austrália, Índia, Singapura, Japão, Brasil, Suíça, Nova Zelândia, Coreia do Sul e Turquia. Declara claramente o que a Cyber Crucible mantém e como a arquitetura sustenta cada regime.

- [A Cyber Crucible está em conformidade com a PIPEDA do Canadá e a Lei 25 de Quebec?](#)
- [A Cyber Crucible está em conformidade com a Lei de Privacidade da Austrália e as APPs?](#)
- [A Cyber Crucible está em conformidade com a Lei de Proteção de Dados Pessoais Digitais da Índia \(DPDP\)?](#)
- [A Cyber Crucible está em conformidade com a PDPA de Singapura?](#)
- [A Cyber Crucible cumpre a APPI do Japão?](#)
- [A Cyber Crucible está em conformidade com a LGPD do Brasil?](#)
- [A Cyber Crucible está em conformidade com a FADP revista da Suíça?](#)
- [A Cyber Crucible está em conformidade com a Privacy Act 2020 da Nova Zelândia?](#)
- [A Cyber Crucible suporta a PIPA da Coreia do Sul?](#)
- [A Cyber Crucible está em conformidade com a KVKK da Turquia?](#)

A Cyber Crucible está em conformidade com a PIPEDA do Canadá e a Lei 25 de Quebec?

Resposta curta: A Cyber Crucible apoia as obrigações de uma organização canadense no âmbito da PIPEDA e da Lei 25 de Quebec principalmente ao processar no endpoint e não coletar conteúdo do cliente, credenciais ou chaves — portanto, há pouca informação pessoal sob sua custódia para proteger, divulgar ou transferir. Ela atua como fornecedora de serviços sob o controle da organização, com um acordo de processamento de dados disponível.

Como se alinha

- **Responsabilidade e salvaguardas.** Criptografia forte, controle de acesso e processamento local apoiam o princípio de salvaguardas de segurança da PIPEDA.
- **Especificidades da Lei 25.** As reformas graduais de Quebec adicionaram a notificação de violações, privacidade por padrão e regras sobre transferências para fora de Quebec; o design sem coleta de dados e com capacidade on-premises apoia as preferências de residência de dados e limita a exposição em transferências.
- **Suporte em caso de violação.** Informações rápidas sobre incidentes ajudam a organização a cumprir os deveres de notificação da PIPEDA e da Lei 25.

O limite honesto

A conformidade é da organização; a Cyber Crucible é um controle e processador de apoio. Ela não possui certificação canadense. Um acordo de processamento de dados e documentação estão disponíveis em dpo@cybercrucible.com.

A Cyber Crucible está em conformidade com a Lei de Privacidade da Austrália e as APPs?

Resposta curta: A Cyber Crucible apoia as obrigações de uma entidade australiana ao abrigo do Privacy Act 1988 e dos Australian Privacy Principles ao minimizar os dados — não recolhe conteúdo de clientes, credenciais ou chaves — e ao processar localmente no endpoint. Isso apoia diretamente o APP 11 (segurança das informações pessoais) e limita a exposição relacionada com a divulgação transfronteiriça ao abrigo do APP 8.

Como se alinha

- **Segurança APP 11** — encriptação, controlo de acesso e proteção autónoma de endpoints.
- **APP 8 transfronteiriço** — a implementação on-premises mantém as informações pessoais na Austrália, quando exigido; nenhum conteúdo de clientes é transferido para o estrangeiro para processamento de segurança.
- **Suporte em caso de violação** — informações sobre o incidente para apoiar as obrigações do regime Notifiable Data Breaches.

Notas para a seleção de fornecedores

O regime de sanções da Austrália para violações graves ou repetidas da privacidade foi substancialmente reforçado, intensificando a análise dos fornecedores. A pegada mínima de dados mantém o lado do fornecedor com baixo risco. A documentação está disponível mediante solicitação.

A Cyber Crucible está em conformidade com a Lei de Proteção de Dados Pessoais Digitais da Índia (DPDP)?

Resposta curta: A Cyber Crucible apoia as obrigações de um fiduciário de dados nos termos da Lei de Proteção de Dados Pessoais Digitais da Índia, atuando como um processador de dados que não recolhe essencialmente dados pessoais e processa no endpoint. Como o conteúdo do cliente nunca é recolhido, as obrigações de consentimento, limitação de finalidade e eliminação têm uma superfície mínima sob a sua custódia.

Como se alinha

- **Papel de processador** sob contrato com o fiduciário de dados.
- **Minimização de dados** — nenhum conteúdo do cliente, credenciais ou chaves são recolhidos.
- **Salvaguardas de segurança e apoio em caso de violação** para as obrigações do fiduciário.

Notas para a seleção de fornecedores

A Índia notificou as Regras DPDP de 2025 em novembro de 2025, com as obrigações substantivas a entrarem em vigor de forma faseada ao longo de aproximadamente os 18 meses seguintes, pelo que os detalhes operacionais (gestão de consentimento, notificação de violações, mecânica de transferências transfronteiriças) ainda estão a entrar em vigor. Entretanto, a implementação no local ("on-premises") apoia as preferências de residência de dados. A Cyber Crucible não detém nenhuma certificação indiana e apoia, em vez de assumir, os deveres do fiduciário. A documentação está disponível mediante pedido.

A Cyber Crucible está em conformidade com a PDPA de Singapura?

Resposta curta: A Cyber Crucible apoia as obrigações de uma organização ao abrigo da Lei de Proteção de Dados Pessoais de Singapura (PDPA) como um intermediário de dados que processa no endpoint e não recolhe conteúdo, credenciais ou chaves do cliente. As obrigações de Proteção e Limitação de Transferência têm pouco a que se aplicar, uma vez que existe uma quantidade mínima de dados pessoais sob a sua custódia.

Como se alinha

- **Papel de intermediário de dados** ao abrigo de um contrato escrito.
- **Obrigações de proteção** — encriptação, controlo de acesso e prevenção no endpoint.
- **Limitação de transferência** — implementação on-premises e nenhuma transferência offshore de conteúdo do cliente para processamento de segurança.

Notas para seleção de fornecedores

A PDPA de Singapura inclui um regime obrigatório de notificação de violações de dados; informação atempada sobre incidentes apoia esse requisito. Um acordo de processamento de dados está disponível mediante pedido.

A Cyber Crucible cumpre a APPI do Japão?

Resposta curta: A Cyber Crucible apoia as obrigações de um operador comercial ao abrigo da Lei de Proteção de Informações Pessoais do Japão (APPI) ao minimizar os dados e o processamento local. Não recolhe conteúdo do cliente, credenciais ou chaves, pelo que as regras de tratamento, fornecimento a terceiros e transferência transfronteiriça têm uma superfície mínima na sua custódia.

Como se alinha

- **Tratamento seguro** — encriptação, controlo de acesso e proteção de endpoints.
- **Transferência transfronteiriça** — a implementação no local (on-premises) apoia a manutenção dos dados pessoais no Japão; nenhum conteúdo do cliente é transferido para o estrangeiro para processamento de segurança.
- **Suporte em caso de violação** — informações sobre incidentes para apoiar as expectativas de reporte da APPI.

Notas para seleção de fornecedores

As alterações à APPI reforçaram o reporte de violações e as regras transfronteiriças; a reduzida pegada de dados mantém as obrigações do fornecedor leves. A documentação está disponível mediante pedido.

A Cyber Crucible está em conformidade com a LGPD do Brasil?

Resposta curta: A Cyber Crucible apoia as obrigações de um controlador nos termos da Lei Geral de Proteção de Dados (LGPD) do Brasil, atuando como operador (processador) que realiza o processamento no endpoint e não coleta conteúdo, credenciais ou chaves do cliente. A maioria das obrigações da LGPD — base legal, direitos dos titulares de dados, regras de transferência — tem superfície mínima, pois há pouco dado pessoal sob sua custódia.

Como se alinha

- **Função de operador** sob contrato, processando conforme as instruções do controlador.
- **Medidas de segurança** — criptografia, controle de acesso e prevenção autônoma no endpoint.
- **Suporte em caso de violação** para os deveres de notificação à ANPD por parte do controlador.

Notas para seleção de fornecedor

A ANPD tem estado cada vez mais ativa em fiscalização e orientações sobre transferência; a implantação on-premises apoia preferências de residência de dados. A Cyber Crucible não possui certificação brasileira e apoia os deveres do controlador. A documentação está disponível mediante solicitação.

A Cyber Crucible está em conformidade com a FADP revista da Suíça?

Resposta curta: A Cyber Crucible apoia as obrigações de uma organização suíça no âmbito da Lei Federal de Proteção de Dados revista (revFADP) ao minimizar os dados e processá-los localmente no endpoint. Como não recolhe conteúdo de clientes, credenciais ou chaves, as obrigações de segurança, registos de processamento e transferência têm uma superfície mínima sob sua custódia.

Como se alinha

- **Função de subcontratante (processor)** ao abrigo de um acordo de processamento de dados.
- **Segurança desde a conceção (security by design)** — a encriptação, o controlo de acesso e a prevenção no endpoint apoiam o dever de segurança de dados da revFADP.
- **Transferência transfronteiriça** — a implementação no local mantém os dados pessoais na Suíça sempre que exigido; estão disponíveis Cláusulas Contratuais-Tipo para transferências.

Notas para seleção de fornecedores

A revFADP alinha-se estreitamente com o RGPD, pelo que grande parte do suporte da Cyber Crucible ao RGPD se aplica também aqui. A documentação, incluindo as SCCs, está disponível mediante pedido.

A Cyber Crucible está em conformidade com a Privacy Act 2020 da Nova Zelândia?

Resposta curta: A Cyber Crucible apoia as obrigações de uma agência da Nova Zelândia ao abrigo da Privacy Act 2020 ao não recolher conteúdo, credenciais ou chaves de clientes, processando os dados no endpoint. Os Information Privacy Principles — em particular armazenamento e segurança (IPP 5) e divulgação transfronteiriça (IPP 12) — têm uma superfície mínima, uma vez que há pouca informação pessoal sob sua custódia.

Como se alinha

- **Segurança IPP 5** — encriptação, controlo de acesso e proteção autónoma do endpoint.
- **IPP 12 transfronteiriço** — a implementação on-premises mantém a informação pessoal na Nova Zelândia; nenhum conteúdo de cliente é transferido para o exterior para processamento de segurança.
- **Suporte a violações** para as obrigações de notificação de violações de privacidade notificáveis da agência.

Notas para seleção de fornecedores

A Privacy Act 2020 introduziu a notificação obrigatória de violações e avisos de conformidade; a informação rápida sobre incidentes apoia ambos. A documentação está disponível mediante pedido.

A Cyber Crucible suporta a PIPA da Coreia do Sul?

Resposta curta: A Cyber Crucible apoia as obrigações de uma organização no âmbito da Lei de Proteção de Informações Pessoais (PIPA) da Coreia do Sul — um dos regimes mais rigorosos a nível global — ao minimizar os dados e o processamento no endpoint. Não recolhe conteúdo de clientes, credenciais ou chaves, pelo que as obrigações de consentimento, tratamento e transferência transfronteiriça têm uma superfície mínima sob a sua custódia.

Como se alinha

- **Função de subcontratante (processor)** sob contrato, seguindo as instruções do responsável pelo tratamento (controller).
- **Salvaguardas robustas** — encriptação, controlo de acesso e prevenção ao nível do endpoint apoiam as exigentes expectativas de segurança da PIPA.
- **Transferência transfronteiriça** — a implementação on-premises apoia a manutenção das informações pessoais na Coreia; nenhum conteúdo de clientes é transferido para o estrangeiro para processamento de segurança.

Notas para a seleção de fornecedores

A PIPA prevê penalizações significativas e requisitos de segurança detalhados; o reduzido volume de dados e a opção on-premises mantêm o risco associado ao fornecedor baixo. A documentação está disponível mediante pedido.

A Cyber Crucible está em conformidade com a KVKK da Turquia?

Resposta curta: A Cyber Crucible apoia as obrigações de um controlador de dados nos termos da Lei de Proteção de Dados Pessoais da Turquia (KVKK) ao não coletar conteúdo de clientes, credenciais ou chaves, e ao processar no endpoint. As obrigações de registro, segurança e transferência têm uma superfície mínima, pois há pouco dado pessoal sob sua custódia.

Como se alinha

- **Papel de processador de dados** sob contrato.
- **Medidas de segurança** — criptografia, controle de acesso e prevenção no endpoint apoiam o requisito de medidas técnicas da KVKK.
- **Transferência transfronteiriça** — a implantação on-premises apoia as preferências de residência de dados sob as regras de transferência da Turquia.

Notas para seleção de fornecedores

O regime de transferência da KVKK e as obrigações de registro no VERBIS competem ao controlador; a Cyber Crucible apoia, e não assume, esses deveres. A documentação está disponível mediante solicitação.