

Guias de Risco de Fornecedores por Estado e Setor nos EUA

Como a Cyber Crucible apoia as leis estaduais de privacidade e segurança dos EUA e as regras setoriais sob a perspectiva de seleção de fornecedores — New York DFS, Califórnia, Texas, Virgínia, Colorado, Massachusetts, Illinois e Pensilvânia. Indica claramente o que a Cyber Crucible detém e não detém.

- [Quais leis estaduais dos EUA sobre privacidade e segurança afetam a seleção de fornecedores de segurança?](#)
- [Como o Cyber Crucible apoia os requisitos de cibersegurança do New York DFS Part 500?](#)
- [Como a Cyber Crucible apoia as obrigações de fornecedores previstas na CCPA/CPRA da Califórnia?](#)
- [Como a Cyber Crucible dá suporte à Texas Data Privacy and Security Act \(TDPSA\)?](#)
- [Como a Cyber Crucible apoia a Lei de Proteção de Dados do Consumidor da Virgínia \(VCDPA\)?](#)
- [Como a Cyber Crucible oferece suporte à Colorado Privacy Act \(CPA\)?](#)
- [Como a Cyber Crucible oferece suporte à Massachusetts 201 CMR 17.00 \(WISP\)?](#)
- [Como a Cyber Crucible aborda a BIPA de Illinois e as preocupações com dados biométricos?](#)
- [Como a Cyber Crucible apoia a lei de notificação de violação da Pensilvânia?](#)
- [Como a Cyber Crucible oferece suporte à Connecticut Data Privacy Act \(CTDPA\)?](#)
- [Como é que a Cyber Crucible apoia a Lei de Privacidade do Consumidor do Utah \(UCPA\)?](#)
- [Como a Cyber Crucible apoia a Lei de Privacidade do Consumidor de Oregon \(OCPA\)?](#)
- [Como a Cyber Crucible apoia a My Health My Data Act de Washington?](#)

- [Como a Cyber Crucible apoia as novas leis estaduais de privacidade de 2025-2026?](#)

Quais leis estaduais dos EUA sobre privacidade e segurança afetam a seleção de fornecedores de segurança?

Resposta curta: Um conjunto crescente e fragmentado de leis estaduais dos EUA impõe obrigações que se estendem aos fornecedores de uma empresa — leis abrangentes de privacidade (Califórnia, Virgínia, Colorado, Texas, entre outras), regras setoriais como o New York DFS Part 500 para o setor financeiro, exigências de segurança de dados como o Massachusetts 201 CMR 17.00, leis sobre dados biométricos como o Illinois BIPA, e estatutos de notificação de violação de dados em todos os estados. O elemento comum é que o comprador deve confirmar que seu fornecedor de segurança minimiza os dados, contrata de forma adequada e protege tudo o que manuseia.

O que essas leis geralmente exigem de um fornecedor

- Um contrato por escrito (acordo de processamento de dados) que limite o fornecedor às instruções do cliente.
- Minimização de dados e limitação de finalidade.
- Salvaguardas de segurança razoáveis e notificação imediata em caso de violação.
- Suporte aos direitos do consumidor (acesso, exclusão) quando dados pessoais forem processados.

Por que a Cyber Crucible atende a isso de forma estrutural

Como a Cyber Crucible nunca coleta conteúdo, credenciais ou chaves do cliente e realiza o processamento no endpoint, as obrigações de maior risco têm pouco a que se aplicar — há uma quantidade mínima de dados pessoais sob sua custódia. Um acordo de processamento de dados e a documentação de suporte estão disponíveis em dpo@cybercrucible.com. As páginas deste livro abordam as regras estaduais específicas que um avaliador tem maior probabilidade de citar.

Como o Cyber Crucible apoia os requisitos de cibersegurança do New York DFS Part 500?

Resposta curta: Para uma instituição financeira abrangida pelo New York DFS Part 500 (23 NYCRR 500), o Cyber Crucible apoia diversos controlos exigidos — autenticação multifator, encriptação, controlos de acesso e resposta a incidentes — ao mesmo tempo que reduz o risco de terceiros, uma vez que nunca recolhe as informações não públicas que a norma protege. O Cyber Crucible é um prestador de serviços terceiro ao abrigo da norma, não uma entidade abrangida em si mesma.

Controlos que apoia

- **Controlos de acesso e MFA** para o painel de gestão, apoiados por autenticação forte.
- **Encriptação** dos dados em trânsito e em repouso.
- **Resposta a incidentes** ao abrigo de um processo documentado de resposta a violações, com um prazo de notificação comprometido disponível por contrato — apoiando a obrigação de notificação de 72 horas do DFS para a entidade abrangida.
- **Redução do risco de terceiros** através da minimização de dados: não são recolhidas informações não públicas.

O limite honesto

As obrigações do Part 500 — a designação de CISO, a avaliação de risco, a certificação anual — recaem sobre a entidade abrangida. O Cyber Crucible fornece evidências de controlo para a política de prestadores de serviços terceiros da entidade (500.11). Não é uma entidade abrangida e não detém qualquer "certificação" Part 500. As evidências são fornecidas ao abrigo de um acordo de confidencialidade (NDA).

Como a Cyber Crucible apoia as obrigações de fornecedores previstas na CCPA/CPRA da Califórnia?

Resposta curta: A Cyber Crucible atua como prestadora de serviços ("service provider") no âmbito da CCPA/CPRA, estando contratualmente obrigada a processar dados apenas de acordo com as instruções do cliente, e não vende nem compartilha informações pessoais. Como praticamente não coleta informações pessoais, as obrigações relativas a direitos do consumidor e tratamento de dados têm alcance muito limitado em sua custódia.

Como isso se alinha

- **Papel de prestadora de serviços** sob um contrato escrito que proíbe o uso secundário.
- **Nenhuma venda ou compartilhamento** de informações pessoais.
- **Apoia os direitos do consumidor** (acesso, exclusão) ao não manter as informações pessoais que, de outra forma, precisariam ser pesquisadas ou excluídas.

Notas para seleção de fornecedores

O California Privacy Rights Act (CPRA) reforçou os termos contratuais para prestadores de serviços e adicionou obrigações relativas a informações pessoais sensíveis; a Cyber Crucible não coleta dados pessoais sensíveis. Um acordo de processamento de dados alinhado à CCPA está disponível mediante solicitação.

Como a Cyber Crucible dá suporte à Texas Data Privacy and Security Act (TDPSA)?

Resposta curta: Sob a Texas Data Privacy and Security Act, a Cyber Crucible atua como processadora vinculada a um contrato de processamento de dados, auxiliando o controlador com solicitações de segurança e de titulares de dados. Seu design de minimização de dados — não coletando conteúdo do cliente, credenciais ou chaves — significa que há poucos dados pessoais a processar, o que simplifica as obrigações do controlador.

Como isso se alinha

- **Papel de processadora** sob um contrato de processamento de dados compatível com a TDPSA.
- **Assistência em segurança e violações de dados** ao controlador.
- **Pegada mínima de dados pessoais**, reduzindo a exposição e o esforço de resposta.

Notas para seleção de fornecedores

A TDPSA se aplica amplamente a empresas que operam no Texas. Como a Cyber Crucible processa essencialmente nenhum dado pessoal e pode ser implantada localmente (on-premises), ela atende tanto às preferências de segurança quanto de residência de dados que um comprador do Texas pode ter. A documentação está disponível mediante solicitação.

Como a Cyber Crucible apoia a Lei de Proteção de Dados do Consumidor da Virgínia (VCDPA)?

Resposta curta: A Cyber Crucible apoia as obrigações de um controlador ao abrigo da VCDPA na qualidade de processador, operando sob um acordo de processamento de dados, ajudando com deveres de segurança de dados e pedidos relativos a direitos do consumidor. O seu design de não recolha significa que retém pouca ou nenhuma informação pessoal, o que mantém baixo o ónus de processamento e resposta do controlador.

Como se alinha

- **Deveres de processador** — assistência em segurança, notificação de violações e avaliações de proteção de dados.
- **Minimização de dados** — nenhum conteúdo de cliente, credenciais ou chaves são recolhidos.
- **Limitação de finalidade** — processamento estritamente de acordo com as instruções do controlador.

Notas para a seleção de fornecedores

A VCDPA exige que os controladores vinculem os processadores por contrato e realizem avaliações para processamentos de maior risco; a reduzida pegada de dados pessoais simplifica ambos os aspetos. Um acordo de processamento de dados está disponível mediante solicitação.

Como a Cyber Crucible oferece suporte à Colorado Privacy Act (CPA)?

Resposta breve: A Cyber Crucible atua como operadora (processor) nos termos da Colorado Privacy Act, vinculada a um acordo de processamento de dados que a obriga a seguir as instruções do controlador, auxiliar na segurança e apoiar os direitos dos consumidores. Como coleta essencialmente nenhum dado pessoal, a maior parte das obrigações da CPA tem alcance mínimo em sua custódia.

Como isso se alinha

- **Papel de operadora (processor)** com processamento contratualmente limitado.
- **Assistência em segurança** e suporte em caso de violação ao controlador.
- **Apoio aos direitos dos consumidores**, por não reter os dados pessoais que, de outra forma, estariam no escopo.

Notas para seleção de fornecedores

A CPA exige avaliações de proteção de dados para processamentos de maior risco e o respeito a mecanismos universais de opt-out no nível do controlador; a pegada mínima mantém o lado do fornecedor simples. A documentação está disponível mediante solicitação.

Como a Cyber Crucible oferece suporte à Massachusetts 201 CMR 17.00 (WISP)?

Resposta curta: A Massachusetts 201 CMR 17.00 exige que qualquer organização que detenha informações pessoais de um residente de Massachusetts mantenha um Written Information Security Program (Programa Escrito de Segurança da Informação) com salvaguardas específicas. A Cyber Crucible apoia o WISP de um cliente com criptografia, controle de acesso e monitoramento — e reduz a exposição do próprio cliente porque essencialmente não detém informações pessoais.

Como isso se alinha

- **Salvaguardas técnicas** — criptografia em trânsito e em repouso, autenticação forte e controle de acesso correspondem aos requisitos do sistema computacional da regulamentação.
- **Proteção e monitoramento de endpoints** apoiam o requisito de software de segurança "razoavelmente atualizado".
- **Footprint mínimo de dados** — as obrigações da regulamentação se aplicam a informações pessoais; a Cyber Crucible não as coleta.

Notas sobre seleção de fornecedores

A 201 CMR 17.00 também exige a supervisão de prestadores de serviços terceirizados por meio de contrato. Um acordo de processamento de dados e a documentação de controles estão disponíveis mediante solicitação.

Como a Cyber Crucible aborda a BIPA de Illinois e as preocupações com dados biométricos?

Resposta curta: A Cyber Crucible não coleta, armazena ou processa identificadores biométricos ou informações biométricas, portanto não gera a exposição que a Lei de Privacidade de Informações Biométricas de Illinois (BIPA) foi concebida para abordar. Não há dados biométricos sob sua custódia para os quais seja necessário obter consentimento, reter ou destruir nos termos da Lei.

Por que não há exposição à BIPA

- **Nenhuma coleta biométrica.** A Cyber Crucible analisa o comportamento de processos e memória, não rostos, impressões digitais ou outros identificadores biométricos.
- **Nenhum dado pessoal sensível.** De forma mais ampla, a Cyber Crucible não coleta dados biométricos, de saúde ou outras categorias especiais de dados.

Observações para seleção de fornecedores

A BIPA é notável por seu direito de ação privado e danos estatutários, o que torna os fornecedores de dados biométricos um foco de escrutínio; a Cyber Crucible simplesmente não se enquadra nessa categoria. Isso pode ser confirmado na documentação de governança de dados disponível mediante solicitação.

Como a Cyber Crucible apoia a lei de notificação de violação da Pensilvânia?

Resposta curta: A Lei de Notificação de Violação de Informações Pessoais da Pensilvânia (73 P.S. §2301, conforme alterada pela Lei 151 de 2022) exige a notificação dos residentes afetados — e, para violações de maior porte, do Procurador-Geral — após uma violação de informações pessoais cobertas. A Cyber Crucible apoia as obrigações de uma organização da Pensilvânia por não armazenar ela própria informações pessoais e por fornecer informações de incidentes rápidas e com qualidade probatória, para que a organização possa cumprir seus prazos legais. A Cyber Crucible tem sede em Pittsburgh, Pensilvânia.

Como isso se alinha

- **Nenhuma informação pessoal armazenada** — a organização mantém o controle sobre qualquer determinação de violação e notificação; não há conjunto de dados do lado do fornecedor a ser perdido.
- **Informações de incidentes rápidas** — o processo de resposta a violações é elaborado para fornecer à organização os fatos necessários para notificar dentro do prazo exigido.
- **Definições ampliadas tratadas** — a emenda de 2022 ampliou as informações pessoais cobertas (incluindo informações médicas e certas combinações de credenciais); o design de não coleta mantém a Cyber Crucible fora dessas categorias.

Notas para seleção de fornecedores

Para violações que afetem mais de 500 residentes da Pensilvânia, a emenda adiciona a notificação ao Procurador-Geral; o papel da Cyber Crucible é apoiar, não determinar, essa obrigação. Detalhes sobre o tratamento de incidentes estão disponíveis mediante acordo de confidencialidade (NDA).

Como a Cyber Crucible oferece suporte à Connecticut Data Privacy Act (CTDPA)?

Resposta curta: A Cyber Crucible atua como operadora (processor) nos termos da Connecticut Data Privacy Act, vinculada por um acordo de tratamento de dados a agir conforme as instruções do controlador e a auxiliar em questões de segurança e em solicitações de titulares de dados. Como não coleta conteúdo de clientes, credenciais ou chaves, a maioria das obrigações da CTDPA tem pouca aplicação em sua custódia.

Como isso se alinha

- **Papel de operadora (processor)** com tratamento contratualmente limitado e o dever de auxiliar o controlador.
- **Minimização de dados** — nenhum conteúdo de clientes, credenciais ou chaves é coletado.
- **Assistência em segurança e suporte em caso de violação** ao controlador.

Observações para seleção de fornecedores

A CTDPA exige que os controladores vinculem os operadores por contrato, respeitem sinais universais de opt-out e realizem avaliações para tratamentos de maior risco; a mínima presença de dados pessoais mantém o lado do fornecedor simples. Um acordo de tratamento de dados está disponível em **dpo@cybercrucible.com**.

Como é que a Cyber Crucible apoia a Lei de Privacidade do Consumidor do Utah (UCPA)?

Resposta breve: A Cyber Crucible atua como responsável pelo tratamento (processor) ao abrigo da Utah Consumer Privacy Act, seguindo as instruções documentadas do controlador no âmbito de um acordo de tratamento de dados. O seu design de não recolha significa que existem poucos dados pessoais sob sua custódia para que as regras de tratamento e divulgação da UCPA se apliquem.

Como se alinha

- **Papel de subcontratante (processor)** ao abrigo de contrato com o controlador.
- **Minimização de dados** — não são recolhidos conteúdos de clientes, credenciais ou chaves.
- **Salvaguardas de segurança** — encriptação, controlo de acessos e prevenção ao nível dos endpoints.

Notas para seleção de fornecedores

A UCPA é geralmente considerada mais orientada para os negócios do que algumas leis estaduais congéneres, mas continua a exigir contratos de subcontratação e segurança razoável; a pegada mínima de dados suporta ambos os requisitos. A documentação está disponível mediante pedido.

Como a Cyber Crucible apoia a Lei de Privacidade do Consumidor de Oregon (OCPA)?

Resposta curta: A Cyber Crucible atua como operadora (processor) nos termos da Lei de Privacidade do Consumidor de Oregon, estando contratualmente vinculada a processar dados apenas conforme as instruções do controlador e a auxiliar em solicitações de segurança e de direitos dos consumidores. Como coleta essencialmente nenhum dado pessoal, a maioria das obrigações da OCPA tem impacto mínimo em sua custódia.

Como está alinhada

- **Deveres da operadora** — auxiliar em segurança, resposta a violações e avaliações de proteção de dados.
- **Minimização de dados** — nenhum conteúdo de clientes, credenciais ou chaves são coletados.
- **Limitação de finalidade** — processamento estritamente conforme as instruções do controlador.

Notas para seleção de fornecedores

A lei de Oregon se destaca por uma definição mais ampla de dados pessoais e por direitos específicos dos consumidores relacionados a terceiros nomeados; a pegada mínima mantém o lado do fornecedor com baixo risco. Um acordo de processamento de dados está disponível mediante solicitação.

Como a Cyber Crucible apoia a My Health My Data Act de Washington?

Resposta curta: A My Health My Data Act de Washington regula de forma abrangente os "dados de saúde do consumidor" e prevê um direito privado de ação, portanto os fornecedores que lidam com esses dados enfrentam exposição real. A Cyber Crucible não coleta dados de saúde do consumidor — ela analisa o comportamento de processos e memória no endpoint e nunca ingere conteúdo do cliente — portanto não cria a superfície de coleta e consentimento que a Lei foi criada para regular.

Por que há pouca superfície de exposição

- **Nenhum dado de saúde do consumidor é coletado.** A Cyber Crucible não reúne conteúdo relacionado à saúde, identificadores ou inferências.
- **Processamento local.** A análise permanece no dispositivo; não há um conjunto de dados de saúde mantido pelo fornecedor.
- **Nenhuma venda ou compartilhamento** de informações pessoais de qualquer tipo.

Notas para seleção de fornecedores

O direito privado de ação previsto na Lei torna os fornecedores de dados de saúde um foco de escrutínio; a Cyber Crucible simplesmente não se enquadra nessa categoria. Isso pode ser confirmado na documentação de governança de dados disponível mediante solicitação. Isto não constitui aconselhamento jurídico — uma entidade abrangida pela lei deve avaliar suas próprias obrigações com o auxílio de assessoria jurídica.

Como a Cyber Crucible apoia as novas leis estaduais de privacidade de 2025–2026?

Resposta curta: Uma onda de leis estaduais abrangentes de privacidade entrou em vigor ao longo de 2025 e 2026 — incluindo New Jersey, Delaware, Iowa, Nebraska, New Hampshire, Tennessee, Minnesota, Maryland e, em 2026, Indiana, Kentucky e Rhode Island. Elas compartilham uma estrutura comum, e o papel de processadora da Cyber Crucible, aliado ao seu design de não coleta, oferece suporte a todas elas da mesma forma: pouco dado pessoal sob custódia, processamento contratualmente limitado e segurança razoável.

A estrutura comum compartilhada por essas leis

- Um contrato de processador obrigatório que limita o fornecedor às instruções da controladora.
- Deveres de minimização de dados e limitação de finalidade.
- Direitos do consumidor (acesso, exclusão, opt-out), cada vez mais com sinais universais de opt-out.
- Salvaguardas de segurança razoáveis e notificação de violação.

Por que uma única resposta cobre o conjunto

Como a Cyber Crucible nunca coleta conteúdo de clientes, credenciais ou chaves, e realiza o processamento no endpoint, as obrigações que variam entre estados — em sua maioria relacionadas ao tratamento e à divulgação de dados pessoais — têm muito pouco a que se vincular. Um único acordo de processamento de dados, consistente, dá suporte a todo o conjunto. A lei de Maryland merece destaque por seu padrão mais rigoroso de minimização de dados, ao qual o design de não coleta atende bem.

O limite honesto

Os limiares estaduais e as datas de vigência mudam, e isto não constitui aconselhamento jurídico; uma controladora deve confirmar quais leis se aplicam a ela. A Cyber Crucible não possui nenhuma "certificação" estadual — ela apoia o cumprimento das obrigações da controladora. A documentação está disponível em **dpo@cybercrucible.com**.