Documentos Legais e de Confiança

Onde encontrar os acordos e a documentação de confiança da Cyber Crucible — NDA mútuo, MSA e EULA, contrato de nível de serviço, acordos de processamento de dados e evidências de conformidade.

Onde posso encontrar os documentos legais e de confiança da Cyber Crucible?

Resposta breve: Os acordos públicos são publicados em cybercrucible.com — o Acordo Mútuo de Confidencialidade (NDA), o MSA e o EULA, o Acordo de Nível de Serviço, a Política de Privacidade e os Termos de Serviço. A documentação de conformidade fornecida mediante solicitação — Cláusulas Contratuais Padrão, Avaliação de Risco de Transferência e Acordos de Processamento de Dados — é obtida através de **dpo@cybercrucible.com**.

Disponível publicamente

Documento	Localização
Acordo Mútuo de Confidencialidade (NDA)	cybercrucible.com/mutualNDA
Contrato Principal de Serviços (MSA) e EULA	cybercrucible.com/msa-and-eula
Acordo de Nível de Serviço	cybercrucible.com/service-level-agreement
Política de Privacidade	cybercrucible.com/privacy-policy
Termos de Serviço	cybercrucible.com/terms-of-service

Fornecido mediante solicitação

Contate **dpo@cybercrucible.com** para obter:

- Cláusulas Contratuais Padrão, incluindo as cláusulas pré-aprovadas pela SDAIA para transferências sauditas
- Avaliação de Risco de Transferência
- Acordo de Processamento de Dados
- Documentação da política de governança e compartilhamento de dados

Estes são fornecidos sujeitos a medidas razoáveis de confidencialidade.

Por que vale a pena ler estes documentos antes da aquisição

Os fornecedores de segurança são incomuns no sentido de que o produto opera com os privilégios mais profundos em seus sistemas, e o contrato rege o que o fornecedor pode fazer com o que vê. Os acordos acima definem ambos. O material de governança de dados, em particular, responde à pergunta que a maioria dos questionários de segurança faz indiretamente: *o que este fornecedor realmente coleta, e para onde isso vai?*

O que é o Cyber Crucible Mutual NDA, e quem está vinculado a ele?

Resposta curta: É um acordo de confidencialidade mútuo e vinculativo que todo funcionário, contratado e fornecedor da Cyber Crucible com potencial acesso a dados operacionais de clientes ou a sistemas de gestão deve assinar **antes do onboarding**. Está publicado em cybercrucible.com/mutualNDA.

Quem assina

Todo o pessoal com potencial acesso a dados operacionais de clientes ou a sistemas de gestão está legalmente vinculado antes do onboarding. Isso inclui funcionários, contratados e fornecedores — não apenas a equipe interna.

Por que "mútuo" importa

Um NDA unilateral protege apenas o fornecedor. Um acordo mútuo vincula a Cyber Crucible a proteger *as suas* informações confidenciais nos mesmos termos que ela espera para as suas próprias. Para um fornecedor de segurança cujo pessoal pode ter acesso a detalhes operacionais do seu ambiente, essa simetria é o ponto central.

Como isso se encaixa nos demais controles

O NDA é a camada contratual de uma postura mais ampla de gestão de riscos internos:

- **Contratual** — NDA mútuo vinculativo antes de qualquer acesso ser concedido.
- **Acesso** — acesso administrativo às instâncias de gestão dos clientes restrito a pessoal previamente avaliado, estritamente com base na necessidade de conhecer, apenas quando exigido para uma operação de negócio ou suporte validada.
- **Desvinculação** — se qualquer fornecedor, prestador, contratado ou funcionário representar um risco de segurança, privacidade ou propriedade intelectual, a Cyber

Crucible gerencia e isola ativamente esse risco ou desvincula imediatamente o recurso.

O NDA estabelece a obrigação. Os controles de acesso limitam o quanto qualquer pessoa poderia fazer mau uso das informações. O mandato de desvinculação é o que torna ambos aplicáveis na prática.

O que abrangem o MSA e o EULA?

Resposta breve: O Master Services Agreement (Contrato Principal de Serviços) rege a relação comercial — serviços, obrigações, responsabilidade e prazo. O End User License Agreement (Contrato de Licença do Utilizador Final) rege a utilização do próprio software, incluindo o âmbito de licenciamento, que se aplica ao código objeto compilado e não ao código-fonte.

Pontos-chave a conhecer antes de assinar

- **Âmbito de licenciamento** — os direitos concedidos aplicam-se à forma de código objeto compilado do software. O contrato não concede direitos para obter ou utilizar o código-fonte.
- **Sem licenças implícitas** — a Cyber Crucible mantém todos os direitos, títulos e interesses sobre os serviços, a documentação e a propriedade intelectual associada. Nada é concedido por implicação.
- **Serviços de implementação** — configuração, personalização, formação de pessoal ou suporte técnico são definidos numa Order Form (Formulário de Encomenda) e não presumidos.
- **Confidencialidade** — ambas as partes podem ter acesso a informações confidenciais da outra parte; cada uma permanece propriedade da parte divulgadora.

Onde consultar

O contrato completo está publicado em cybercrucible.com/msa-and-eula. Esta página é um resumo orientativo, não um substituto — o contrato publicado prevalece.

O que o Acordo de Nível de Serviço cobre?

Resposta curta: O SLA define os compromissos de serviço que a Cyber Crucible assume perante os clientes — disponibilidade, capacidade de resposta do suporte e os termos associados. Está publicado em cybercrucible.com/service-level-agreement.

Como o SLA se relaciona com o design do produto

Vale a pena notar para quem está a avaliar: como a prevenção ocorre de forma autónoma no endpoint, tipicamente em menos de 200 milissegundos, a proteção não depende da disponibilidade do serviço da forma como um produto de análise em nuvem depende.

Um endpoint cujo servidor de gestão esteja inacessível — ou que esteja deliberadamente isolado (air-gapped) — continua totalmente protegido. A avaliação de ameaças e a interdição de processos são locais. A disponibilidade do plano de gestão afeta a geração de relatórios e a administração, não a defesa.

Esta é uma distinção significativa ao comparar SLAs entre fornecedores. Para uma ferramenta dependente da nuvem, o tempo de inatividade do plano de gestão pode significar proteção reduzida ou inexistente. Aqui, não é o caso.

Onde ler

O acordo completo está disponível em cybercrucible.com/service-level-agreement. Os compromissos de capacidade de resposta do suporte e quaisquer termos específicos do ambiente devem ser confirmados com o seu representante da Cyber Crucible.

Como faço para preencher um questionário de segurança ou uma avaliação de risco de fornecedor para o Cyber Crucible?

Resposta curta: A maioria das perguntas é respondida pelo material de governança de dados — o que é coletado, o que nunca é coletado, como é protegido em trânsito, onde é processado e quais modelos de implantação estão disponíveis. Para qualquer coisa que exija documentação assinada, entre em contato com **dpo@cybercrucible.com**.

As respostas que a maioria dos questionários exige

Pergunta típica	Onde é respondida
Quais dados de clientes o fornecedor coleta?	*Quais dados o Cyber Crucible coleta — e quais nunca coleta?*
Os dados são compartilhados com ou vendidos a terceiros?	*O Cyber Crucible vende ou compartilha dados de clientes com terceiros?*
Como os dados são criptografados em trânsito?	*Como os dados do Cyber Crucible são protegidos em trânsito?*
Onde os dados são processados e armazenados?	*Onde meus dados são processados, e podem permanecer dentro do meu país?*
Subprocessadores e controles da cadeia de suprimentos?	*Como o Cyber Crucible gerencia o risco da cadeia de suprimentos e de ameaças internas?*
Componentes de código de terceiros ou estrangeiros?	*O Cyber Crucible incorpora bibliotecas de terceiros ou código estrangeiro?*
Função de controlador ou operador de dados?	*O Cyber Crucible é um controlador de dados ou um operador de dados?*

Pergunta típica	Onde é respondida
Mecanismo de transferência de dados transfronteiriça?	*Como as transferências de dados transfronteiriças são tratadas?*

Duas respostas que costumam surpreender os avaliadores

Sobre certificações: o programa de segurança do Cyber Crucible está alinhado com estruturas do setor reconhecidas, mas **atualmente não possui certificação ISO 27001 ou SOC 2**. Se o seu processo exigir evidências certificadas, levante essa questão logo no início, e não mais tarde.

Sobre divulgação de dados: como chaves de criptografia, credenciais e arquivos de clientes nunca são coletados, não há nada nessas categorias para divulgar a qualquer parte — inclusive sob processo legal. Vários itens do questionário sobre divulgação, retenção e exclusão são respondidos pela ausência de coleta, e não por um controle.

Qualquer coisa não coberta

Entre em contato com **dpo@cybercrucible.com** informando o requisito específico, sua jurisdição e qual modelo de implantação você está avaliando.