

# 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).

---

Revision #1

Created 2026-07-24 06:04:28 UTC by Dennis Underwood

Updated 2026-07-24 06:04:28 UTC by Dennis Underwood