¿Cómo respalda Cyber Crucible los requisitos de ciberseguridad de la Parte 500 del NY DFS?

Respuesta breve: Para una institución financiera sujeta a la Parte 500 del NY DFS (23 NYCRR 500), Cyber Crucible respalda varios controles requeridos —autenticación multifactor, cifrado, controles de acceso y respuesta a incidentes— a la vez que reduce el riesgo de terceros, ya que nunca recopila la información no pública que la norma protege. Cyber Crucible es un proveedor de servicios externo bajo la norma, no una entidad cubierta en sí misma.

Controles que respalda

- **Controles de acceso y MFA** para el panel de administración, respaldados por una autenticación sólida.
- **Cifrado** de los datos en tránsito y en reposo.
- **Respuesta a incidentes** bajo un proceso documentado de respuesta a brechas, con un plazo de notificación comprometido disponible por contrato, lo que respalda la obligación de notificación de 72 horas del DFS para la entidad cubierta.
- **Reducción del riesgo de terceros** mediante la minimización de datos: no se recopila información no pública.

El límite honesto

Las obligaciones de la Parte 500 —designación de un CISO, evaluación de riesgos, la certificación anual— recaen en la entidad cubierta. Cyber Crucible proporciona evidencia de controles para la política de proveedores de servicios externos de la entidad (500.11). No es una entidad cubierta y no posee ninguna "certificación" de la Parte 500. La evidencia se proporciona bajo un acuerdo de confidencialidad (NDA).

Revision #1
Created 2026-07-24 02:05:43 UTC by Dennis Underwood
Updated 2026-07-24 02:05:43 UTC by Dennis Underwood