

A Cyber Crucible possui um plano de recuperação de desastres e continuidade de negócios?

Resposta curta: Sim. A Cyber Crucible mantém um plano de recuperação de desastres testado, de responsabilidade da gestão de TI, e uma arquitetura construída para alta disponibilidade. Como a prevenção de ameaças é executada localmente no endpoint, a proteção do endpoint continua mesmo durante uma interrupção do backend de gestão.

Resiliência por arquitetura

O backend de gestão é construído com armazenamento redundante e replicado, de modo que a perda de um nó individual não causa perda de dados ou indisponibilidade. O Acordo de Nível de Serviço publicado compromete-se com 99,9% de disponibilidade mensal para o backend de gestão e relatórios, excluindo manutenções programadas e causas fora de controle razoável. A proteção do endpoint em si não é afetada por uma interrupção do backend.

Backups e planejamento de contingência

Os dados são continuamente replicados e copiados para armazenamento externo seguro, utilizando credenciais privilegiadas distintas, com os backups protegidos contra ransomware por meio de tratamento offline ou imutável, e testados regularmente. O plano mantém um plano de resposta a emergências informáticas, um plano de sucessão, um estudo de criticidade de dados e uma lista de criticidade de serviços, e incorpora análise de impacto nos negócios, estratégias de recuperação, um plano de comunicação que inclui notificação aos clientes, e objetivos de recuperação definidos. Os testes incluem exercícios de simulação (table-top) e simulações de recuperação.

Alinhamento com frameworks e o limite honesto

O plano está alinhado com a NIST SP 800-34 e com a ISO/IEC 27001:2022 A.5.29–A.5.30. A Cyber Crucible define objetivos de ponto de recuperação e tempo de recuperação para o backend; os valores-alvo específicos, bem como o plano em si, são disponibilizados aos avaliadores sob acordo de confidencialidade (NDA). Como a proteção é executada localmente, a defesa do endpoint continua com praticamente nenhuma lacuna de tempo de recuperação durante uma interrupção do backend ou em uma implantação isolada (air-gapped).

Revision #1

Created 2026-07-24 23:37:07 UTC by Dennis Underwood

Updated 2026-07-24 23:37:07 UTC by Dennis Underwood