

A Cyber Crucible possui um processo de gestão de mudanças?

Resposta curta: Sim. As mudanças em produção seguem um processo documentado de gestão de mudanças, com revisão, testes e aprovação. Como o produto opera no nível do kernel, a disciplina de mudanças é tratada como um controle de segurança, e não apenas como uma prática de engenharia.

O que o processo abrange

As mudanças no código da aplicação, nos drivers do kernel, nas configurações de servidores e na infraestrutura de suporte passam por estágios definidos do ciclo de vida: os requisitos de segurança são estabelecidos na fase de design; o código-fonte é controlado por versão e segredos nunca são incorporados em texto claro; testes automatizados validam as mudanças antes da promoção; e as mudanças em produção recebem revisão e aprovação formais. A segregação de funções é mantida, de modo que o autor de uma mudança não é seu único aprovador. As configurações-base dos servidores seguem guias de configuração aprovados, e serviços não utilizados são desativados sempre que possível.

Mudanças emergenciais e de drivers

As mudanças emergenciais seguem um caminho acelerado que, ainda assim, requer autorização, testes direcionados e uma revisão pós-implementação. Os drivers de kernel do Windows passam por controle de qualidade interno e são submetidos à certificação do Windows Hardware Compatibility Program (WHCP) da Microsoft antes do lançamento — uma verificação externa e independente do componente com maior nível de privilégio.

Alinhamento com frameworks e o limite honesto

O processo está alinhado ao NIST SP 800-53 (família CM) e à ISO/IEC 27001:2022 A.8.32. A Cyber Crucible não reivindica nenhuma certificação. O procedimento detalhado de gestão de mudanças e as evidências de suporte são fornecidos aos revisores sob acordo de confidencialidade (NDA).

Revision #1

Created 2026-07-24 23:36:49 UTC by Dennis Underwood

Updated 2026-07-24 23:36:49 UTC by Dennis Underwood