Análise de riscos

Descrição dos Planos de Contenção e Contingência

1. Autenticação Forte e Bloqueio de Conta:
   * Contenção: A autenticação de dois fatores e limites de tentativas de login reduzem o risco de invasões. Caso haja muitas tentativas de acesso, implementar CAPTCHA e alertas de segurança.
   * Contingência: Bloquear temporariamente contas afetadas e entrar em contato com o usuário para redefinição de senha.
2. Sanitização e Filtragem de Dados para Injeção de SQL e XSS:
   * Contenção: Sanitizar entradas de usuários para evitar a execução de comandos SQL ou scripts maliciosos. Implementar bibliotecas de segurança que escapem automaticamente consultas SQL.
   * Contingência: Configurar backups frequentes para restaurar o banco de dados em caso de um ataque bem-sucedido e revisar dados comprometidos.
3. Criptografia e HTTPS para Proteção de Dados:
   * Contenção: Utilizar criptografia AES para dados sensíveis e protocolos HTTPS para todas as comunicações.
   * Contingência: Se houver vazamento de dados, notificar os usuários afetados, investigar o impacto e revisar todas as políticas de armazenamento.
4. Moderação Automática e Revisão de Avaliações:
   * Contenção: Implementar moderação automática que filtra conteúdo ofensivo ou spam, permitindo que usuários denunciem avaliações inadequadas.
   * Contingência: Caso a moderação não detecte um problema, revisar manualmente avaliações e ajustar as regras de filtro conforme necessário.
5. Proteção contra DDoS e Infraestrutura Redundante:
   * Contenção: Usar firewalls de aplicação, sistemas de detecção de intrusão e CDNs com proteção contra DDoS para reduzir a exposição a ataques.
   * Contingência: Redirecionar tráfego para servidores secundários e informar aos usuários sobre o status de manutenção durante ataques.
6. Backups e Alta Disponibilidade:
   * Contenção: Configurar backups automáticos e alta disponibilidade, com failover para servidores de backup em caso de falhas.
   * Contingência: Utilizar backups para restaurar dados e funções críticas do sistema rapidamente. Enviar notificações aos usuários se o tempo de inatividade ultrapassar um limite aceitável.
7. Conformidade com LGPD/GDPR:
   * Contenção: Garantir que as políticas de coleta e armazenamento de dados estejam em conformidade com LGPD/GDPR, incluindo solicitações de consentimento.
   * Contingência: Suspender temporariamente o processamento de dados em caso de descobertas de não conformidade e realizar auditoria completa para evitar multas e penalidades.

Identificação dos riscos:

* Desfalque de membros da equipe
* Problemas com hardware
* Problemas com software
* Alterações na demanda do cliente