

CYBER NEWS

O Boletim Informativo Oficial de Gestão de Riscos em Terceiros



NESTA EDIÇÃO

Gerenciamento de resposta a incidente e Teste de Penetração

- **Por que fazer gestão de incidente e Teste de Penetração?**
- **Boas Práticas de Gestão de incidente e Teste de Penetração**
- **Práticas que devem ser exigidas na gestão de incidente e Teste de Penetração**
- **Benefícios de exigir gestão de incidente e Teste de Penetração**

CONCLUSÃO

Gerenciar respostas a incidentes e realizar testes de penetração regularmente reduz riscos, assegura conformidade e protege os serviços. Este boletim reforça a importância dessas práticas e orienta provedores sobre boas condutas.

Por que fazer gestão de incidente e Teste de Penetração?

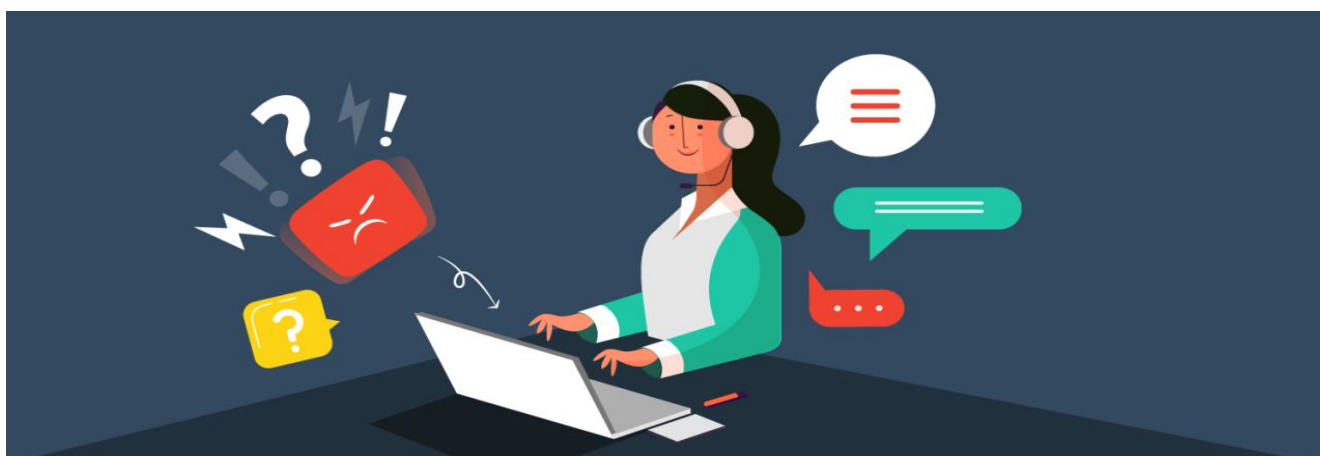
- Garantir a continuidade e segurança dos serviços críticos.
- Reduzir riscos operacionais, financeiros e reputacionais.
- Assegurar conformidade com legislações, normas e requisitos regulatórios.
- Aumentar a visibilidade sobre vulnerabilidades e acessos aos dados, sistemas e informações da empresa.

Boas práticas de gestão de incidente e Teste de Penetração

- Antes da implementação – realizar análise de riscos técnicos, regulatórios e operacionais, além de verificar histórico de segurança e conformidade.
- Durante a operação – monitorar continuamente vulnerabilidades, executar testes de penetração e acompanhar indicadores de resposta a incidentes.
- Após o incidente – remover acessos indevidos, validar correções aplicadas, garantir destruição segura de dados quando necessário e avaliar a eficácia das medidas adotadas.

📄 Práticas que devem ser exigidas na gestão incidente e Teste de Penetração:

- Política formal de resposta a incidentes documentada e aprovada.
- Plano de comunicação para reporte rápido de incidentes críticos.
- Execução periódica de testes de penetração com escopo definido e relatórios detalhados.
- Correção tempestiva das vulnerabilidades identificadas nos testes.
- Monitoramento contínuo de segurança para detecção de ameaças.
- Registro e análise de incidentes anteriores para melhoria contínua.
- Treinamento das equipes envolvidas em resposta a incidentes e testes.
- Gestão de acessos para evitar privilégios excessivos ou indevidos.
- Validação da destruição segura de dados após incidentes ou término de contrato.
- Controle sobre subcontratados garantindo que sigam as mesmas práticas de segurança.
- Auditorias regulares para verificar conformidade com normas e requisitos regulatórios.
- Relatórios de vulnerabilidade e mitigação compartilhados com o contratante.
- Testes pós-correção para confirmar que as falhas foram eliminadas.
- Simulações de incidentes (exercícios de resposta)



🕒 Benefícios de exigir gestão de incidente e Teste de Penetração:

- ✓ Redução de riscos cibernéticos e prevenção de ataques.
- ✓ Maior eficácia na resposta a incidentes, minimizando impactos.
- ✓ Ambiente mais seguro e resiliente contra vulnerabilidades.
- ✓ Conformidade com normas e legislações de segurança da informação.
- ✓ Transparência sobre vulnerabilidades e correções aplicadas.
- ✓ Proteção de dados sensíveis e continuidade dos serviços críticos.
- ✓ Melhoria contínua da postura de segurança por meio de testes regulares

📌 Conclusão

Uma gestão estruturada de resposta a incidentes e a realização periódica de testes de penetração são fundamentais para garantir segurança, continuidade e qualidade dos serviços.

Ao exigir que fornecedores adotem essas práticas e também as estendam aos seus terceiros, a organização fortalece todo o ecossistema, reduz vulnerabilidades e aumenta a confiabilidade dos processos.