VERITAS

RECUPERE COM CONFIANÇA

Implemente um plano que não deixe dúvidas sobre recuperação.

Evite os danos que o tempo de inatividade e o roubo de dados podem causar. Prepare-se hoje para a resiliência de amanhã com nossa lista de verificação de recuperação cibernética.

FASE 1

Fase 1 | 30 dias

Estabeleça a Base.
O que você pode fazer AGORA para proteger sua empresa.

- Crie políticas de proteção e retenção para todas as cargas de trabalho.
- Use armazenamento imutável.
- Implemente a estratégia de backup 3-2-1 – três cópias em dois formatos; uma fora do local, incluindo um air gap virtual e/ou físico; o isolamento de SaaS é vital.
- Aplique controles de segurança (por exemplo, MFA, MPA, segmentação de rede, RBAC, criptografia).
- Considere appliances reforçados específicos.
- Habilite a detecção de anomalias com base em IA.
- Ative a detecção de malware e as regras de retenção.
- Atualize o software e os patches de segurança (em andamento).

FASE 2

Fase 2 | 60 dias

Gerencie proativamente os riscos.
Foco em pessoas, processos e tecnologia.

- Identifique ativos críticos "ausentes".
- Realize a avaliação de dados obscuros.
- Descubra e classifique dados confidenciais.
- Identifique e monitore comportamentos de alto risco dos usuários finais.
- Crie um ambiente de recuperação isolado (IRE ou sala limpa).
- Desenvolva runbooks de recuperação, priorizando a ordem das operações.
- Integre com a SecOps e estabeleça manuais de resposta a incidentes (por exemplo, Integração SIEM/SOAR/XDR).

FASE 3

Fase 3 | 90 dias

Refinar. Ensaiar. Adaptar.

- Ajuste as políticas de proteção de dados para ter 100% de sucesso no backup, de acordo com SLAs.
- Ajuste a detecção de anomalias com base em IA (elimine falsos positivos/negativos).
- Realize exercícios de mesa, incluindo ensaios de recuperação sem interrupções.
- Ensaie a recuperação e valide os resultados.

Veja a lista de verificação completa de recuperação cibernética >

VERITAS

1 (866) 837-4827 ▪ www.veritas.com/pt/br