Guia de segurança contra ransomware

Reduzir risco de indisponibilidade e extorsão.

Como usar

Percorra os itens com os responsáveis. Marque a situação, registre evidências e priorize as ações não atendidas. Revise após mudanças relevantes.

Controle / ação	Situação	Evidência / ação
01. Manter patches e MFA	Sim / Parcial / Não	_____
02. Restringir privilégios e acesso remoto	Sim / Parcial / Não	_____
03. Treinar contra phishing	Sim / Parcial / Não	_____
04. Isolar cópias de backup	Sim / Parcial / Não	_____
05. Monitorar alertas	Sim / Parcial / Não	_____
06. Acionar equipe em suspeita e preservar evidências	Sim / Parcial / Não	_____
07. Testar recuperação em ambiente seguro	Sim / Parcial / Não	_____

Próximos passos

Registre responsável e prazo para os itens prioritários; valide a conclusão com evidências. Não inclua credenciais nem dados pessoais desnecessários. Material de orientação, não certificação.

Da orientação à execução

1. Reduza exposição

Priorize atualizações, MFA em e-mail e acessos remotos, privilégios mínimos e segmentação de rede. Remova serviços desnecessários expostos à internet.

2. Prepare a recuperação

Mantenha cópias separadas das credenciais da operação. Teste restauração de arquivos e sistemas críticos; registre duração e integridade.

3. Responda com segurança

Em suspeita, isole os ativos afetados conforme plano interno e preserve logs. Acione a equipe de resposta; evite alterações que comprometam evidências.

4. Retome de forma controlada

Valide ambiente limpo, rotacione credenciais comprometidas e restaure a partir de cópias verificadas. Avalie obrigações de comunicação e registre lições aprendidas.

Registre responsáveis, prazos e evidências. Material orientativo; adapte à realidade da organização.