

Sua empresa sobrevive a um ransomware?

10 perguntas para conferir se o backup da empresa traz a operação de volta depois de um ataque. Marque só o que você consegue comprovar hoje.

1. Leia e marque

Marque a caixa quando a resposta for "sim" e você souber provar.

2. Some as marcas

Anote o total no fim da lista, na página 3.

3. Veja o resultado

A interpretação e por onde começar estão na página 3.

O checklist itens 1 a 3

☐**01 Regra 3-2-1**

Existem pelo menos 3 cópias dos dados importantes, em 2 tipos de mídia, com 1 delas fora do escritório?

Se o servidor e o HD de backup ficam na mesma sala e na mesma rede, um único incidente (ransomware, incêndio, furto, pico de energia) leva tudo junto. A cópia fora do escritório é a que sobra.

☐**02 Cópia imutável ou offline**

Pelo menos uma das cópias é imutável (ninguém consegue alterar ou apagar por um período) ou fica desconectada da rede?

Grupos de ransomware procuram e apagam os backups antes de criptografar os arquivos. Uma cópia imutável ou desligada da rede não pode ser apagada nem com a senha do administrador.

☐**03 Teste de restauração**

Nos últimos 3 meses, alguém restaurou de verdade um arquivo, uma pasta ou uma máquina a partir do backup e conferiu que abriu?

Backup que nunca foi restaurado é uma suposição, não uma garantia. O teste mostra se a cópia está íntegra e quanto tempo a volta realmente leva.



04 Backup do Microsoft 365

Os e-mails, o OneDrive, o SharePoint e o Teams têm backup fora do ambiente da Microsoft?

A Microsoft mantém o serviço no ar, mas a lixeira e a retenção padrão têm prazo e não são uma cópia independente. Exclusão por engano, conta invadida ou ex-funcionário que apaga tudo pedem um backup próprio.



05 Retenção

O backup guarda versões antigas por tempo suficiente (por exemplo, 30 dias ou mais) para voltar a um ponto anterior ao ataque?

O ransomware pode ficar semanas escondido antes de agir. Se o backup guarda só os últimos dias, todas as versões disponíveis podem já estar contaminadas.



06 MFA no console de backup

O acesso ao painel do backup exige autenticação em dois fatores (MFA) e usa uma conta separada da conta de administrador do dia a dia?

Quem invade a rede tenta entrar no console do backup para apagar as cópias e desligar as rotinas. MFA e uma conta exclusiva fecham essa porta.



07 Tempo de volta (RTO e RPO)

A empresa definiu quanto tempo pode ficar parada (RTO) e quantas horas de trabalho pode perder (RPO), e o backup foi configurado para isso?

Backup uma vez por dia significa perder até um dia de trabalho. Restaurar um servidor inteiro pela internet pode levar horas. Esses números devem ser uma decisão da empresa, não uma surpresa no dia do problema.



08 Responsável pelo backup

Há uma pessoa ou empresa responsável por acompanhar o backup, que recebe os alertas de falha e age sobre eles?

Rotina de backup falha em silêncio: disco cheio, senha trocada, agente parado. Sem alguém olhando os alertas, a falha só aparece no dia em que a cópia é necessária.



09 Criptografia das cópias

As cópias são criptografadas, inclusive as que ficam na nuvem ou em HD externo?

Um HD de backup perdido ou uma cópia vazada expõe dados de clientes e funcionários, com consequências também na LGPD. Com criptografia, a cópia sem a chave não serve a ninguém.



10 Plano de resposta

Existe um plano escrito para um ataque: quem chamar, o que desligar, por onde começar a restaurar e como avisar clientes?

Na hora do ataque não há tempo para decidir do zero. Um plano de uma página, com contatos e prioridades, encurta a parada e evita erros como religar máquinas infectadas.

Como ler o resultado



Total de caixas marcadas: ____ de 10

Conte só o que você consegue comprovar hoje, não o que "deve estar funcionando".

9 ou 10 marcadas

Boa base

O backup da empresa tem o que precisa para voltar depois de um ataque. Mantenha os testes de restauração e revise o plano de resposta uma vez por ano.

6 a 8 marcadas

Atenção

Há pontos que podem impedir a volta da operação. Comece pelos itens sem marca entre o 2, o 3 e o 6: são os que um ataque explora primeiro.

5 ou menos

Risco alto

Hoje um ransomware provavelmente pararia a empresa por dias, com risco de perder dados para sempre. Priorize uma cópia imutável fora da rede e um teste de restauração.

Por onde começar. Os itens 2 (cópia imutável ou offline) e 3 (teste de restauração) pesam mais que os outros. Se um deles ficou sem marca, trate como prioridade, mesmo que o total tenha sido alto. Depois, siga pelos itens sem marca na ordem da lista.

Backup Acronis com a TechPartners BR

A TechPartners BR revende, implanta e acompanha o backup Acronis: licenças na medida do que precisa ser protegido, rotinas e retenção configuradas, acompanhamento das falhas, testes periódicos de restauração e backup do Microsoft 365 fora do ambiente da Microsoft. Contratação mensal ou anual, o que for melhor para a empresa.

Quer revisar os itens sem marca com quem faz isso todo dia? Peça um levantamento do backup da sua empresa.

Telefone e WhatsApp

+55 11 4118-1992

E-mail

contato@techpartnersbr.com

Backup Acronis

techpartnersbr.com/backup-acronis.html

Diagnóstico online de TI (gratuito)

techpartnersbr.com/materiais/diagnostico-de-ti.html

Falar com a equipe no WhatsApp

Material informativo da TechPartners BR, outubro de 2026. Não substitui uma avaliação técnica do ambiente. Atendemos empresas de todo o Brasil; sede na Rua Amazonas, 439, Conj. 63, São Caetano do Sul/SP.