

CHECKLIST · BACKUP

O backup da sua empresa **volta** quando você precisa?

Um checklist para descobrir se o seu backup resiste a falha de hardware, erro humano e ransomware, e as perguntas certas para fazer ao seu fornecedor.

Regra 3-2-1-1-0

Ransomware

Perguntas ao fornecedor

A REFERÊNCIA

A regra 3-2-1-1-0

A regra 3-2-1 de backup ganhou dois números por causa do ransomware, que hoje procura e apaga as cópias antes de pedir o resgate.

NÚMERO	O QUE SIGNIFICA	POR QUE IMPORTA
3	Três cópias dos dados	Uma falha não leva tudo
2	Dois tipos de armazenamento	Um defeito de mídia não leva tudo
1	Uma cópia fora da empresa	Incêndio, roubo ou enchente não levam tudo
1	Uma cópia imutável	Ransomware e erro humano não apagam essa cópia
0	Zero erros nos testes de restauração	Você sabe que o backup volta antes de precisar

Imutável é a cópia gravada de um jeito que não pode ser alterada nem apagada durante o período de retenção: nem pelo administrador, nem por um invasor com a senha dele, nem por um ransomware.

ONDE ESTÁ O SEU RISCO

Os três cenários mais comuns

HD externo ou NAS na mesma sala: se o problema for incêndio, roubo ou ransomware, o backup vai junto com o servidor.

Backup em nuvem sincronizado: se a cópia for acessível com as mesmas senhas, o ataque pode atingi-la também.

Backup que nunca foi restaurado: o job diz "concluído", mas ninguém sabe se os dados voltam íntegros.

CHECKLIST

O seu backup **resiste?**

Marque o que é verdade hoje.

☐ Sabemos exatamente o que é copiado: servidores, ERP, banco de dados, arquivos.
Inclusive Microsoft 365 ou Google Workspace, se a empresa usa.

☐ A cópia é feita pelo menos uma vez por dia, sem depender de alguém lembrar.

☐ Existe uma cópia fora do prédio da empresa.

☐ Uma das cópias é imutável.
Ninguém consegue alterar nem apagar durante a retenção.

☐ A cópia externa usa credenciais separadas do ambiente principal.

☐ Os dados são criptografados na transferência e no armazenamento.

☐ Sabemos por quanto tempo as cópias ficam guardadas (retenção).

☐ A restauração foi testada nos últimos 3 meses, e deu certo.

☐ Alguém é avisado quando uma rotina de backup falha.

☐ Os dados ficam no Brasil, o que simplifica a LGPD.

Perguntas para fazer ao seu fornecedor

☐ Onde ficam as cópias e quem tem acesso a elas?

☐ Existe cópia imutável? Por quanto tempo?

☐ Quem faz a restauração quando eu precisar, e em quanto tempo?

COMO A DATA COR RESOLVE

A cópia que **nenhum ataque** apaga

Backup em nuvem com cópia diária fora da empresa, em data center próprio no Brasil, e backup imutável: a cópia não pode ser alterada nem apagada durante a retenção, nem por um ransomware. A cópia imutável pode ficar na DATA COR ou em outra cidade da nossa rede, e o ambiente é compatível com Veeam.

Restauração testada com frequência, monitoramento NOC 24x7 e custo mensal em reais.

[Fale com um especialista no WhatsApp](#)

(18) 3304-0700

[Conheça o backup imutável](#)datacor.com.br