

Segurança e backup do Microsoft 365

12 itens para conferir se o ambiente da empresa está protegido contra conta invadida, vazamento e exclusão sem volta. 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 de 12 na página 3.

3. Veja o resultado

A interpretação e por onde começar estão na página 3.

O checklist itens 1 a 3

**01 MFA para todos**

Todos os usuários entram no Microsoft 365 com um segundo fator (aplicativo no celular), ligado pelos padrões de segurança ou por regras de acesso condicional?

Senha vazada é a porta de entrada mais comum em contas do Microsoft 365. Os padrões de segurança do Microsoft Entra ID ligam o MFA para todos sem custo extra. O acesso condicional permite regras mais finas, mas exige o Entra ID P1, incluído no Business Premium.

**02 Autenticação antiga bloqueada**

Nenhum programa, impressora ou sistema ainda entra no e-mail só com usuário e senha (POP, IMAP, SMTP com autenticação básica)?

Esses acessos não pedem o segundo fator e anulam o MFA. Os padrões de segurança bloqueiam a autenticação herdada. Liste os scanners e sistemas que enviam e-mail e troque para um método moderno antes que parem.

**03 Poucos administradores**

Há de 2 a 4 administradores globais, cada um com conta própria, separada da conta usada no dia a dia?

Conta de administrador usada para ler e-mail e navegar é o alvo preferido do phishing. A Microsoft recomenda menos de cinco administradores globais. Dê a cada técnico só a função de que ele precisa (usuários, Exchange, cobrança).



04 Conta de emergência

Existe uma conta de acesso de emergência, com senha longa guardada em cofre e protegida por uma chave de segurança física, para o caso de o administrador principal ficar sem acesso?

Sem ela, perder o celular do único administrador pode trancar a empresa fora do próprio ambiente. Monitore qualquer uso dessa conta.



05 Convidados revisados

Alguém revisa a lista de convidados externos pelo menos a cada trimestre, remove quem não trabalha mais com a empresa e limita quem pode convidar?

Convidados de projetos antigos continuam com acesso a equipes do Teams e a pastas do SharePoint até alguém removê-los.



06 Compartilhamento externo

O compartilhamento externo do SharePoint e do OneDrive está no nível que a empresa precisa, com links "Qualquer pessoa" desligados ou com data de validade?

O link "Qualquer pessoa" funciona sem login: se o e-mail com o link for encaminhado, o arquivo vai junto. Os níveis vão de "Qualquer pessoa" a "Somente pessoas da organização". Para a maioria das empresas, "Convidados novos e existentes" com validade nos links basta.



07 Encaminhamento automático

O encaminhamento automático de e-mails para endereços de fora da empresa está bloqueado, ou liberado só para quem precisa?

Quem invade uma caixa costuma criar uma regra que copia tudo para fora, em silêncio. A política padrão de spam de saída do Exchange Online bloqueia esse encaminhamento. Confira se ninguém liberou para todos.



08 Saída de funcionário

Há um roteiro de desligamento: bloquear o login, encerrar as sessões, converter a caixa em compartilhada se precisar e transferir o OneDrive antes de excluir o usuário?

Excluir o usuário apaga o OneDrive dele depois do prazo de retenção (30 dias por padrão). Bloquear e transferir antes evita perder arquivos e acesso indevido de quem saiu.



09 Prazos de retenção conhecidos

A empresa sabe por quanto tempo o Microsoft 365 guarda o que é excluído (tabela da página 4) e decidiu se isso basta?

Cada serviço tem o seu prazo, e os padrões são curtos. Políticas de retenção do Microsoft Purview podem guardar por mais tempo, mas retenção não é backup: não devolve uma pasta inteira ao estado de ontem com um clique.



10 Backup independente

E-mails, OneDrive, SharePoint e Teams têm backup fora do ambiente da Microsoft, com retenção definida pela empresa?

É a cópia que sobra quando a exclusão passa do prazo da lixeira, quando uma conta invadida apaga tudo ou quando um ransomware criptografa os arquivos sincronizados no OneDrive.



11 Teste de restauração

Nos últimos 3 meses, alguém restaurou do backup uma caixa de e-mail, uma pasta do SharePoint ou um arquivo do OneDrive e conferiu o resultado?

Backup sem teste é suposição. O teste mostra se as contas novas entraram no backup e quanto tempo a volta leva.



12 Domínio protegido contra falsificação

O domínio de e-mail tem SPF, DKIM e DMARC, com o DMARC já em quarentena ou rejeição?

Sem isso, qualquer um pode mandar e-mail "em nome" da empresa para clientes e fornecedores. Faça o teste gratuito em techpartnersbr.com/materiais/teste-email-falsificado.html.

Como ler o resultado



Total de caixas marcadas: ____ de 12

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

11 ou 12 marcadas

Boa base

O ambiente tem as proteções principais. Revise convidados, administradores e o teste de restauração a cada trimestre.

8 a 10 marcadas

Atenção

Há brechas que um ataque comum explora. Comece pelos itens sem marca entre o 1, o 3 e o 10.

7 ou menos

Risco alto

Uma conta invadida ou uma exclusão por engano hoje pode custar e-mails e arquivos sem volta. Priorize MFA para todos e um backup independente.

Por onde começar. Os itens 1 (MFA para todos), 3 (poucos administradores) e 10 (backup independente) 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.

O que o Microsoft 365 não guarda por você

A Microsoft mantém o serviço no ar. Os dados, os acessos e a cópia independente são da empresa: é o modelo de responsabilidade compartilhada.

A Microsoft cuida

- Data centers, servidores e rede
- Disponibilidade do serviço
- Cópias internas para falha de hardware
- Correções e atualizações da plataforma

A sua empresa cuida

- Quem acessa e como (contas, MFA, administradores)
- Compartilhamento, convidados e retenção configurados
- Os próprios dados: exclusão por engano, por quem saiu ou por invasor
- Uma cópia independente e o teste de restauração

Por quanto tempo dá para recuperar o que foi excluído

O quê	Prazo padrão
E-mail excluído (Exchange Online)	Fica em Itens Excluídos até a pasta ser esvaziada; depois, 14 dias em Itens Recuperáveis (o administrador pode aumentar para até 30).
Arquivos do SharePoint e do OneDrive	Lixeira de até 93 dias, somando o primeiro e o segundo estágio.
OneDrive de usuário excluído	30 dias por padrão (o administrador pode mudar o prazo).
Usuário excluído	30 dias para restaurar a conta.
Grupo do Microsoft 365 ou equipe do Teams excluída	30 dias para restaurar.
Conversas do Teams	Não há lixeira: passado o "Desfazer" logo depois de apagar, a mensagem só pode ser recuperada pelo administrador, pela pesquisa do Microsoft Purview, se houver política de retenção ou retenção legal.

Backup Acronis para Microsoft 365

A TechPartners BR revende, implanta e acompanha o backup Acronis para Microsoft 365: cópia de Exchange Online, OneDrive, SharePoint e Teams fora do ambiente da Microsoft, com retenção definida pela empresa, restauração de itens individuais e testes periódicos.

Telefone e WhatsApp

+55 11 4118-1992

E-mail

contato@techpartnersbr.com

Backup Acronis

techpartnersbr.com/backup-acronis.html

Materiais gratuitos

techpartnersbr.com/materiais-gratuitos.html

Prazos padrão conforme a documentação da Microsoft em outubro de 2026; o administrador pode alterar alguns deles e a Microsoft pode mudá-los. 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.