

TI para escritórios de contabilidade

12 itens sobre LGPD, proteção, backup, e-mail, acessos, certificados digitais e as máquinas antes do fechamento do mês. 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 4.

3. Veja o resultado

A interpretação e por onde começar estão na página 4.

O checklist itens 1 a 3

☐**01** LGPD **Dados dos clientes mapeados**

O escritório sabe onde ficam os dados pessoais dos clientes e dos funcionários deles (folha, documentos, declarações) e quem tem acesso a cada pasta?

A LGPD pede saber o que se guarda, para quê e quem acessa. Pastas por cliente, abertas só para a equipe que atende, reduzem vazamento interno e facilitam responder a um pedido de titular.

☐**02** LGPD **Responsável e plano para incidente**

Há uma pessoa responsável pela proteção de dados, um canal para pedidos de titulares e um roteiro do que fazer se houver vazamento?

Num incidente com risco aos titulares, a lei prevê comunicação à ANPD e aos afetados. Decidir quem faz o quê antes evita imprevisto no pior dia.

☐**03** Proteção **Antivírus com EDR em todas as máquinas**

Todas as máquinas, inclusive os notebooks de quem trabalha de casa, têm proteção corporativa com detecção e resposta (EDR), gerenciada num painel e com alguém acompanhando os alertas?

Antivírus gratuito, cada um de um jeito e sem ninguém olhando, avisa tarde. O EDR registra o que aconteceu na máquina e ajuda a parar um ataque antes que ele chegue ao servidor.



04 Backup Backup do sistema contábil testado

O banco de dados do sistema contábil e fiscal e as pastas dos clientes têm backup automático, com uma cópia fora do escritório, e alguém testou a restauração nos últimos 3 meses?

Restaurar o banco de dados do sistema é diferente de restaurar um arquivo: precisa ser testado com o sistema abrindo. Faça o teste antes do fechamento, não durante.



05 E-mail Equipe atenta ao phishing

A equipe sabe reconhecer e-mail falso com boleto, guia, intimação ou "pendência na Receita", e tem a quem perguntar antes de clicar?

Escritório contábil recebe documentos de muitos remetentes todos os dias, o que facilita o golpe. Uma regra simples (na dúvida, pergunte antes) evita a maior parte dos casos.



06 E-mail SPF, DKIM e DMARC no domínio

O domínio do escritório tem SPF, DKIM e DMARC, para que ninguém mande boleto ou guia falsa "em nome" do escritório aos clientes?

Os clientes confiam no e-mail do escritório, e o golpista sabe disso. Faça o teste gratuito em techpartnersbr.com/materiais/teste-email-falsificado.html.



07 E-mail MFA no e-mail e nos sistemas na nuvem

O e-mail e os sistemas na nuvem pedem um segundo fator (código ou aprovação no celular) para todos?

Com o MFA, a senha vazada sozinha não abre a caixa. É a proteção mais barata contra conta invadida.



08 Acessos Cada um com o seu acesso

Cada pessoa tem o seu usuário no Windows, no sistema contábil e nos portais, sem senha compartilhada, e o acesso de quem sai é retirado no mesmo dia?

Senha compartilhada impede saber quem fez o quê e continua funcionando depois que a pessoa sai do escritório.



09 Certificados Inventário dos certificados digitais

Há uma lista dos certificados digitais do escritório e dos clientes, com tipo (A1 ou A3), titular, vencimento, onde está guardado e quem pode usar?

Certificado vencido no dia da entrega trava a obrigação. Saber quais existem e quando vencem permite renovar com antecedência.



10 **Certificados** Certificados A1 protegidos

Os certificados A1 (arquivo .pfx) ficam instalados só nas máquinas necessárias, com senha forte, fora de pastas compartilhadas e de e-mails, e os tokens A3 têm guarda definida?

O A1 é um arquivo: copiado junto com a senha, permite assinar em nome do cliente de qualquer computador. Trate como a chave do cofre.



11 **Máquinas** Atualizações longe do fechamento

As atualizações do Windows e dos programas são instaladas numa janela combinada, longe da semana do fechamento e dos prazos de entrega?

Atualização que reinicia a máquina ou muda o sistema no dia da entrega é risco desnecessário. Deixe a semana do fechamento estável e atualize logo depois.



12 **Máquinas** Máquinas prontas para o pico

Antes do fechamento, alguém confere espaço em disco, nobreak, impressoras, certificados que vencem no mês e se ainda há máquina com Windows 10 sem atualização de segurança?

O Windows 10 está sem suporte gratuito desde 14/10/2025. Máquina sem correção de segurança, disco cheio ou nobreak sem bateria costumam aparecer justamente na semana de mais trabalho.

Na semana antes do fechamento

Seis conferências rápidas para a TI não atrapalhar as entregas. Não entram na soma do checklist.



Backup da noite

Confira que o backup da noite anterior terminou sem erro, inclusive o do banco do sistema contábil.



Certificados do mês

Veja quais certificados vencem nos próximos 30 dias e avise os clientes.



Atualizações antes

Instale o que estiver pendente antes da semana do fechamento e adie reinícios para depois das entregas.



Espaço em disco

Servidor e máquinas com folga de espaço: banco de dados cheio para no pior momento.



Nobreak e impressoras

Teste o nobreak e confira toner e scanner antes do pico.



Suporte à mão

Telefone e canal de chamado do suporte de TI anotados para a equipe.

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 escritório tem as proteções principais. Mantenha o teste de restauração e a revisão dos certificados como rotina mensal.

8 a 10 marcadas

Atenção

Há pontos que podem parar o escritório num fechamento ou expor dados de clientes. Comece pelos itens sem marca entre o 3, o 4 e o 10.

7 ou menos

Risco alto

Um ataque ou uma falha comum hoje pode parar as entregas e expor dados de clientes. Priorize backup testado, EDR e a guarda dos certificados.

Por onde começar. Os itens 3 (EDR), 4 (backup testado) e 10 (certificados AI protegidos) pesam mais que os outros: são os que um ataque usa para parar o escritório ou agir em nome dos clientes. Depois, siga pelos itens sem marca na ordem da lista.

TI para escritório contábil com a TechPartners BR

A TechPartners BR construiu a experiência atendendo escritórios contábeis. O suporte de TI cuida das máquinas, das atualizações e dos programas do dia a dia; o backup Acronis protege os dados com testes periódicos de restauração; e o Microsoft 365 é administrado e licenciado via CSP.

Quer revisar os itens sem marca com quem faz isso todo dia? Peça uma conversa com a equipe.

Telefone e WhatsApp

+55 11 4118-1992

E-mail

contato@techpartnersbr.com

Suporte de TI

techpartnersbr.com/suporte-de-ti.html

Materiais gratuitos

techpartnersbr.com/materiais-gratuitos.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.