trinity ti
GESTÃO INTEGRADA EM T.I.

MATERIAL GRATUITO · TRINITY TI

Checklist LGPD para Contadores

12 verificações objetivas para descobrir, em menos de 20 minutos, se o seu escritório contábil está em conformidade com a LGPD e protegido contra vazamento de dados, ransomware e fraude por email.

COMO USAR ESTE MATERIAL

Antes de tudo: por que um contador precisa disso?

O seu escritório contábil é, simultaneamente, controlador e operador de dados pessoais de centenas de clientes — pessoas físicas e empresas. Para a ANPD (Autoridade Nacional de Proteção de Dados), isso significa obrigações claras de segurança, governança e prestação de contas, com multas que podem chegar a 2% do faturamento (limite de R$ 50 milhões por infração).

Mas LGPD para contador não é só política e termo no papel. A conformidade real depende de tecnologia funcionando: backup confiável, MFA em todas as contas, criptografia, controle de acesso, DLP no email, retenção e descarte automatizados.

Este Checklist foi escrito por quem implanta esses controles no dia a dia — não por advogado, não por consultor genérico. É a lista que a Trinity TI usa internamente quando faz diagnóstico de TI para escritórios contábeis no Rio de Janeiro.

COMO USAR

1. Reserve 20 minutos com o responsável pela TI do escritório (interno ou terceirizado).
2. Percorra os 12 pontos abaixo. Marque ✔ para CONFORME, ■ para PARCIAL e ✗ para AUSENTE.
3. Some os pontos AUSENTES e PARCIAIS — esses são os riscos a tratar primeiro.
4. Use o mini-glossário no final se algum termo não estiver claro.
5. Se quiser revisar o resultado com um especialista, fale com a Trinity TI — conversa gratuita.

BACKUP E RECUPERAÇÃO

01 — Backup automático e imutável (à prova de ransomware)

☐ CONFORME ☐ PARCIAL ☐ AUSENTE

O QUE É

Todos os arquivos do escritório (sistema fiscal, SharePoint/OneDrive, contratos, folha) têm cópia de segurança automática diária, em nuvem, criptografada e imutável (WORM). Ransomware não consegue apagar o backup.

COMO VERIFICAR

Pergunte: quando foi a última restauração de teste? Se a resposta for 'nunca' ou 'não sei', o ponto é AUSENTE — backup que nunca foi restaurado não conta como backup.

RISCO SE AUSENTE

Sem isso: um único ataque de ransomware paralisa o escritório por dias e pode causar perda definitiva de acervo no meio de um fechamento de IR ou SPED.

AUTENTICAÇÃO

02 — MFA (autenticação em dois fatores) em 100% das contas

☐ CONFORME ☐ PARCIAL ☐ AUSENTE

O QUE É

Todas as contas de email corporativo, sistema fiscal, internet banking, sistemas de cliente e portais governamentais exigem segundo fator (app autenticador, SMS, biometria ou token físico) — não apenas senha.

COMO VERIFICAR

Liste as contas dos sócios, contadores e estagiários. Para cada uma: Microsoft 365 ✔/✗, banco ✔/✗, e-CAC/eSocial ✔/✗, sistema contábil ✔/✗. Uma só conta sem MFA já é uma porta aberta.

RISCO SE AUSENTE

Sem isso: roubo de uma única senha (phishing) dá acesso total à caixa de email do contador — e o golpista começa a enviar boletos falsos para os clientes do escritório.

CRIPTOGRAFIA

03 — Criptografia em repouso e em trânsito

☐ CONFORME ☐ PARCIAL ☐ AUSENTE

O QUE É

Os arquivos que contêm dados pessoais (CPF, RG, folha, IR, contratos sociais) ficam armazenados em pastas criptografadas, e qualquer transmissão (email, upload, acesso remoto) usa TLS/HTTPS. Notebooks da equipe têm disco criptografado (BitLocker ou similar).

COMO VERIFICAR

Pegue um notebook de colaborador. Tente acessar o disco fora do Windows (via USB de boot). Se conseguir ler os arquivos, AUSENTE. Olhe se SharePoint/OneDrive estão configurados e ativos no escritório (não Drive/Dropbox pessoal de cada um).

RISCO SE AUSENTE

Sem isso: notebook perdido, roubado ou descartado expõe a base inteira de clientes. Caso típico de incidente reportável à ANPD.

GOVERNANÇA DE PASTAS

04 — SharePoint / OneDrive corporativo com permissões controladas

☐ CONFORME ☐ PARCIAL ☐ AUSENTE

O QUE É

Os documentos do escritório ficam em ambiente corporativo (Microsoft 365 SharePoint ou Google Workspace Drive Corporativo), organizados por cliente, com permissões granulares — cada colaborador vê apenas o que precisa. Pen drives e Drive pessoal são proibidos.

COMO VERIFICAR

Liste 5 ex-colaboradores que saíram do escritório no último ano. Os acessos deles foram revogados em até 24h da saída? As pastas dos clientes deles foram redistribuídas formalmente?

RISCO SE AUSENTE

Sem isso: ex-funcionário leva a base de clientes para a concorrência, ou colaborador atual acessa folha e dados sigilosos sem necessidade.

EMAIL E ANTI-FRAUDE

05 — DLP no email (Data Loss Prevention)

☐ CONFORME ☐ PARCIAL ☐ AUSENTE

O QUE É

O servidor de email tem regras que detectam e bloqueam o envio externo de CPF, RG, números de conta bancária e folha de pagamento em anexo, e marcam emails com dados sensíveis. Reduz drasticamente o risco de vazamento por erro humano.

COMO VERIFICAR

Pergunte ao TI: 'temos regra de DLP no Exchange / Google Workspace para CPF e dados financeiros?'. Se não souber responder com clareza, o ponto é AUSENTE.

RISCO SE AUSENTE

Sem isso: um anexo enviado por engano para o cliente errado vira incidente LGPD. Acontece com frequência maior do que se imagina.

EMAIL E ANTI-FRAUDE

06 — Anti-phishing avançado e proteção contra BEC

☐ CONFORME ☐ PARCIAL ☐ AUSENTE

O QUE É

O email corporativo tem filtros avançados contra phishing (links maliciosos, anexos perigosos) e contra Business Email Compromise — a tentativa de se passar por sócio ou cliente para enganar a equipe a alterar boleto ou transferir valores.

COMO VERIFICAR

Pergunte à equipe: quantos emails suspeitos vocês recebem por semana? Existe canal para reportar? Já houve treinamento simulado de phishing nos últimos 12 meses?

RISCO SE AUSENTE

Sem isso: o famoso golpe do 'boleto trocado' — golpista invade conta do contador, envia boleto falso para o cliente, valor cai em conta laranja. Perda média no Brasil: R$ 35 mil por incidente.

ENDPOINT

07 — Antivírus corporativo gerenciado (EDR) em todos os equipamentos

☐ CONFORME ☐ PARCIAL ☐ AUSENTE

O QUE É

Todos os computadores e notebooks da equipe têm antivírus de classe empresarial (com EDR — detecção e resposta), gerenciado de forma centralizada por console. Não é Windows Defender solto nem antivírus gratuito.

COMO VERIFICAR

Abra a console do antivírus. Há quantas máquinas? É o mesmo número de computadores do escritório? Quando foi o último incidente detectado? Atualizações automáticas estão em dia em todas as máquinas?

RISCO SE AUSENTE

Sem isso: malware se espalha pelo escritório inteiro a partir de uma única máquina infectada. EDR detecta padrões de ransomware antes da criptografia em massa.

REDE

08 — Firewall corporativo e segmentação de rede

☐ CONFORME ☐ PARCIAL ☐ AUSENTE

O QUE É

A rede do escritório tem firewall corporativo (Sophos, Fortinet, Mikrotik etc.) com IPS/IDS, filtro de conteúdo e segmentação: rede de visitantes/Wi-Fi separada da rede de produção; servidores em segmento isolado. Não é apenas o roteador da operadora.

COMO VERIFICAR

Conecte um celular no Wi-Fi do escritório. Você consegue acessar a pasta compartilhada do servidor? Se sim, AUSENTE — visitante não pode pingar produção.

RISCO SE AUSENTE

Sem isso: um celular comprometido de visitante (ou cliente) tem acesso direto aos servidores do escritório.

ACESSO REMOTO

09 — VPN para acesso remoto e home office contábil

☐ CONFORME ☐ PARCIAL ☐ AUSENTE

O QUE É

Quando contador, sócio ou estagiário acessam o sistema fiscal ou as pastas do escritório de fora (home office, viagem), é por VPN corporativa autenticada — não por desktop remoto exposto na internet nem por compartilhamento improvisado.

COMO VERIFICAR

Pergunte: como o pessoal acessa quando trabalha de casa? Se a resposta envolve 'AnyDesk', 'RDP direto' ou 'compartilhei a senha do servidor', AUSENTE.

RISCO SE AUSENTE

Sem isso: serviços expostos na internet são o vetor #1 de ataque a empresas pequenas e médias no Brasil. Scanners automáticos varrem 24h.

GOVERNANÇA LGPD

10 — DPO (Encarregado de Dados) designado e canal LGPD ativo

☐ CONFORME ☐ PARCIAL ☐ AUSENTE

O QUE É

O escritório tem um Encarregado pelo Tratamento de Dados Pessoais (DPO) formalmente designado — pode ser interno ou contratado — e um canal claro (email ou formulário no site) para que titulares de dados façam solicitações (acesso, correção, exclusão).

COMO VERIFICAR

Visite o site do escritório. Existe página/seção 'LGPD' ou 'Privacidade' com o nome e contato do DPO? Existe email do tipo dpo@escritorio.com.br? Se não, AUSENTE.

RISCO SE AUSENTE

Sem isso: descumprimento direto da LGPD (Art. 41). É um dos primeiros pontos checados em fiscalização da ANPD.

RETENÇÃO E DESCARTE

11 — Política de retenção e descarte de documentos

☐ CONFORME ☐ PARCIAL ☐ AUSENTE

O QUE É

Existe regra clara — e tecnicamente implementada — de por quanto tempo cada tipo de documento é mantido (folha, IR, contratos, emails) e como é descartado quando o prazo vence. Não é um documento engavetado; está configurado no Microsoft 365 / sistema fiscal.

COMO VERIFICAR

Pergunte: emails de 8 anos atrás de cliente que não é mais do escritório ainda estão na caixa? Pastas de clientes inativos há mais de 5 anos ainda estão online? Se sim, AUSENTE.

RISCO SE AUSENTE

Sem isso: guardar dados além do necessário aumenta a superfície de risco em caso de vazamento e descumpre o princípio de necessidade da LGPD (Art. 6º, III).

PESSOAS

12 — Treinamento periódico em segurança e LGPD

☐ CONFORME ☐ PARCIAL ☐ AUSENTE

O QUE É

Toda a equipe (sócios, contadores, estagiários, recepção) recebe treinamento anual sobre segurança, phishing, manuseio de dados pessoais e procedimentos LGPD. Treinamento é documentado e tem lista de presença / certificado.

COMO VERIFICAR

Olhe a pasta de RH. Existem registros de treinamento de segurança e LGPD assinados pela equipe nos últimos 12 meses? Estagiários novos recebem o conteúdo na entrada?

RISCO SE AUSENTE

Sem isso: a tecnologia mais cara não para um clique errado. 90% dos incidentes começam em erro humano. Sem cultura, não há controle que segure.

REFERÊNCIA RÁPIDA

Mini-glossário para contadores.

Os termos técnicos do checklist, traduzidos para o dia a dia do escritório contábil.

MFA

Multi-Factor Authentication (Autenticação de Múltiplos Fatores). Exige um segundo fator além da senha — código no celular, biometria ou token. Mata 99% dos ataques de roubo de senha.

DLP

Data Loss Prevention (Prevenção de Perda de Dados). Tecnologia que detecta e bloqueia o envio de dados sensíveis (CPF, conta bancária, folha) para fora da organização, geralmente no email.

WORM

Write Once, Read Many. Backup imutável — depois de gravado, não pode ser apagado ou alterado, nem pelo administrador. Defesa primária contra ransomware.

EDR

Endpoint Detection and Response. Geração atual de antivírus corporativo, com inteligência para detectar comportamento malicioso (não só assinaturas de vírus conhecidos).

DPO

Data Protection Officer (Encarregado pelo Tratamento de Dados). Pessoa designada pelo escritório como ponto de contato com titulares e ANPD. Obrigatório pela LGPD (Art. 41).

BEC

Business Email Compromise. Tipo de fraude em que o golpista assume (ou se passa por) uma conta de email corporativo para enganar a equipe — geralmente para desviar pagamentos.

SharePoint

Plataforma da Microsoft (parte do Microsoft 365) para armazenamento corporativo de arquivos com controle granular de permissão, retenção e versionamento. Equivalente Google: Drive Compartilhado.

ANPD

Autoridade Nacional de Proteção de Dados. Autarquia federal responsável por fiscalizar a LGPD e aplicar sanções administrativas (advertência, multa, bloqueio de tratamento, etc.).

RPO / RTO

Recovery Point Objective (quanto de dado posso perder) e Recovery Time Objective (quanto tempo posso ficar sem operar). Métricas que orientam o desenho do backup e do plano de continuidade.

Ransomware

Tipo de ataque em que arquivos do escritório são criptografados pelo invasor, que cobra resgate para liberar. Pagar o resgate raramente resolve — backup imutável é o que protege de verdade.

PRÓXIMO PASSO

Achou pontos AUSENTES ou PARCIAIS?

Conversemos por 30 minutos — sem custo.

A Trinity TI é um MSP fundado em 2005, no Rio de Janeiro, especializado em gestão integrada de tecnologia para escritórios contábeis, advocacia, clínicas e cartórios — organizações que lidam com dados sensíveis e operam sob exigência regulatória.

Marque uma conversa de 30 minutos com um dos nossos consultores. Você passa pelos pontos que ficaram em vermelho no seu checklist, recebe o diagnóstico técnico do que prioriza primeiro e leva embora — sem custo e sem compromisso — um plano de adequação proporcional ao porte do seu escritório.

Falar com a Trinity TI

Site	trinityti.com.br/lps/contabilidade
WhatsApp	(21) 4062-7800 · wa.me/552140627800
Telefone	(21) 4062-7800 — seg. a sex., 8h às 18h
E-mail	contato@trinityti.com

BÔNUS · PROGRAMA DE INDICAÇÃO PARA CONTADORES

Contadores percebem antes de todo mundo quando o cliente não tem backup, MFA ou TI estruturada. A Trinity TI tem um programa simples de indicação: condições especiais para o seu cliente e um reconhecimento para o escritório que indicou. Pergunte no WhatsApp.

© 2026 Trinity Tecnologia e Informática Ltda. · Material gratuito · Distribuição livre.